ULTIMATE Q/A AWS SAA-C02

Solutions Architect Associate

Questions

Luca Cesarano
https://lucacesarano.com

Table of Contents

Set of Questions #1

Questions from 1-100

Question #1

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).
Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Commented [LC1]: ANSWER

Question #2

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.
Which EC2 configuration meets these requirements?

A. Launch the EC2 instances in a cluster placement group in one Availability Zone.
B. Launch the EC2 instances in a spread placement group in one Availability Zone.
C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

Commented [LC2]: Cluster Placement Group is made for instances that needs to be close to each other with very low network overhead

Question #3

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world.
Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.
What should a solutions architect do to accomplish this?

A. Use Amazon S3 with Transfer Acceleration to host the application.
B. Use Amazon S3 with CacheControl headers to host the application.
C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Commented [LC3]: TL;DR: CloudFront is for content delivery. S3 Transfer Acceleration is for faster transfers and higher throughput to S3 buckets (mainly uploads). Amazon S3 Transfer Acceleration is an S3 feature that accelerates uploads to S3 buckets using AWS Edge locations - the same Edge locations as in AWS CloudFront service

Question #4

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.
Which service should the solutions architect use?

A. Amazon Elastic File System (Amazon EFS)
B. Amazon FSx
C. Amazon S3
D. AWS Storage Gateway

Commented [LC4]: "Windows" is the key, FSx is the best replacement with Windows instances that need a network drive.

Question #5

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.
How should a solutions architect integrate the microservices?

A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2.
B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.
D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Commented [LC5]: That's how basic decoupling of applications work.

Question #6

A company captures clickstream data from multiple websites and analyses it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.
Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

A. Amazon EC2
B. AWS Lambda
C. Amazon Kinesis Data Streams
D. Amazon Kinesis Data Firehose
E. Amazon Kinesis Data Analytics

Commented [LC6]: Answer is C,D. A doesn't make sense. Lambda as well since the maximum time per lambda is 15 mins. E is also not needed since they're asking for streaming data.

Answer is C, D.
C. streams the data from the source to AWS, can stream even gigabyte per second. D helps with moving the data to a destination like Redshift.

Question #7

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.
What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

A. Configure an Amazon CloudFront distribution in front of the ALB.
B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Commented [LC7]: A,D are OUT.
C is better than B because the action is taken BEFORE the CPU utilization peaks, which may be ideal in this case.

Question #8

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.
Which architecture should the solutions architect implement? (Choose two.)

A. Add AWS Shield.
B. Add Aurora Replica.
C. Add AWS Direct Connect.
D. Add AWS Global Accelerator.
E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

Commented [LC8]: For the DB, B is the best option

Commented [LC9]: For the web tiers, CF is the best option

Question #9

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.
What should the solutions architect do to separate the read requests from the write requests?

A. Enable read-through caching on the Amazon Aurora database.
B. Update the application to read from the Multi-AZ standby instance.
C. Create a read replica and modify the application to use the appropriate endpoint.
D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Commented [LC10]: ANSWER

Question #10

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity.
Which solution will meet these requirements?

A. AWS Direct Connect for both the initial transfer and ongoing connectivity.
B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity.
C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.
D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity.

Commented [LC11]: ANSWER

Question #11

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.
Which action will meet these requirements?

A. Modify the ALB security group to deny incoming traffic from blocked countries.
B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.
C. Use Amazon CloudFront to serve the application and deny access to blocked countries.
D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

Commented [LC12]: ANSWER

Question #12

A company is creating a new application that will store a large amount of data. The data will be analysed hourly and modified by several Amazon EC2 Linux instances that are deployed across multiple Availability Zones. The application team believes the amount of space needed will continue to grow for the next 6 months.
Which set of actions should a solutions architect take to support these needs?

A. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the application instances.
B. Store the data in an Amazon Elastic File System (Amazon EFS) file system. Mount the file system on the application instances.
C. Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access to the application instances.
D. Store the data in an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS volume shared between the application instances.

Commented [LC13]: B is good because it can be shared by many instances plus it can easily grow with a few clicks.

Question #13

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours.
Which solution will improve the performance of the application when it is moved to AWS?

A. Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.
B. Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.
C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.
D. Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Commented [LC14]: Dynamo is out of scope. DB on EC2 is never a choice since Amazon provides its DBs services. C is correct because read replicas are needed here to lower read I/O ops.

Question #14

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.
Which storage solution should the solutions architect use?

A. EBS Amazon Elastic Block Store (Amazon EBS)
B. Amazon EC2 instance store
C. Amazon Elastic File System (Amazon EFS)
D. Amazon S3

Commented [LC15]: B. It requires Block storage, it's not a problem if one instance exits, supports very high speed.

Question #15

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.
Which action should the solutions architect take to accomplish this?

A. Generate presigned URLs for the files.
B. Use cross-Region replication to all Regions.
C. Use the geoproximity feature of Amazon Route 53.
D. Use Amazon CloudFront with the S3 bucket as its origin.

Commented [LC16]: It says "static". CF + S3 are the best choice.

Question #16

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.
Which combination of AWS services would meet these requirements? (Choose two.)

A. AWS Fargate
B. AWS Lambda
C. Amazon DynamoDB
D. Amazon EC2 Auto Scaling
E. MySQL-compatible Amazon Aurora

Commented [LC17]: ANSWER

Question #17

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.
What should a solutions architect do to accomplish this?

A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.
D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy. Create alias records in Route 53 that point to the Application Load Balancer.

Commented [LC18]: A can't do that plus we lose features of the ALB. B can't do that. D is wrong because the weighted policy doesn't guarantee that requests goes in base of locations.

C is the best.

Question #18

A solutions architect is designing a solution to access a catalogue of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images.
What is the MOST cost-effective solution to meet these requirements?

A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
C. Use AWS Lambda to manipulate the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
D. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Commented [LC19]: Answer is B. C is wrong, you can't store images in DynamoDB. A,D are wrong because of EC2 which is not the best choice.

Question #19

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data multiple AWS Regions.
How should a solutions architect design the S3 solution?

A. Create an additional S3 bucket in another Region and configure cross-Region replication.
B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Commented [LC20]: ANSWER

Question #20

A company has application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications.
Which action will fulfill these requirements and maintain security?

A. Configure an S3 interface endpoint.
B. Configure an S3 gateway endpoint.
C. Create an S3 bucket in a private subnet.
D. Create an S3 bucket in the same Region as the EC2 instance.

Commented [LC21]: ANSWER

Question #21

A company`s web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, Accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.
What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

A. Create a read replica and direct reporting traffic to the replica.
B. Create a Multi-AZ database and direct reporting traffic to the standby.
C. Create a cross-Region read replica and direct reporting traffic to the replica.
D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Commented [LC22]: ANSWER

Question #22

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.
Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Choose two.)

A. Amazon S3 for cold data storage
B. Amazon Elastic File System (Amazon EFS) for cold data storage
C. Amazon S3 for high-performance parallel storage
D. Amazon FSx for Lustre for high-performance parallel storage
E. Amazon FSx for Windows for high-performance parallel storage

Commented [LC23]: S3 is good for hold cold data

Commented [LC24]: FSx for Lustre is made for HPC applications

Question #23

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.
Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

A. Detach a volume on an EC2 instance and copy it to Amazon S3.
B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.
C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.
D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.
E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

Commented [LC25]: That's the second phase

Commented [LC26]: That's the first phase

To copy a ec2 machine in another region: first, you create an AMI, then, you copy an AMI to another region; finally, you launch an instance from an AMI in the other region

Question #24

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet.
What should the solutions architect do to accomplish this? (Choose two.)

A. Create a route table entry for the endpoint.
B. Create a gateway endpoint for DynamoDB.
C. Create a new DynamoDB table that uses the endpoint.
D. Create an ENI for the endpoint in each of the subnets of the VPC.
E. Create a security group entry in the default security group to provide access.

Commented [LC27]: A gateway endpoint is used to avoid using Internet ports for connecting to S3 or DynamoDB.

After creating the Gateway Endpoint, you need to add in the route table an entry related to the endpoint

Question #25

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted.
How should this be accomplished?

A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
C. Take a Snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Commented [LC28]: ANSWER

Question #26

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.
Which solution would be MOST efficient?

A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon Elastic Block Store (Amazon EBS).
C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon Elastic File System (Amazon EFS).
D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Commented [LC29]: ANSWER

Question #27

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow.
Which set of actions will improve website performance for users worldwide?

A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register instances with the same ALB using cross- Region VPC peering.
D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Commented [LC30]: ANSWER

Question #28

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API. The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.
Which solution should the solutions architect suggest?

A. Set up an Amazon API Gateway and use Amazon ECS.
B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
C. Set up an Amazon API Gateway and use AWS Lambda functions.
D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling.

Commented [LC31]: ANSWER

Question #29

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.
Which pricing model should the company choose?

A. Reserved Instances
B. Spot Block Instances
C. On-Demand Instances
D. Scheduled Reserved Instances

Commented [LC32]: D is not available anymore. B is not available anymore. A is wrong because Reserved Instances are always available while here we need them only for 7 days / month.

C is the answer.

Commented [LC33]: SPOT BLOCK are not available anymore. Scheduled Reserved Instances are not available anymore.

Question #30

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.
What should a solutions architect do to meet these requirements? (Choose two.)?

A. Increase the number of EC2 instances.
B. Decrease the number of EC2 instances.
C. Configure a Network Load Balancer in front of the EC2 instances.
D. Configure an Application Load Balancer in front of the EC2 instances.
E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Commented [LC34]: C better than D because it's level-4

Commented [LC35]: Classic high availability solution

Question #31

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups.
What should be done to enable encryption for future backups?

A. Enable default encryption for the Amazon S3 bucket where backups are stored.
B. Modify the backup section of the database configuration to toggle the Enable encryption check box.
C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.
D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance.

Commented [LC36]: Similar to a previous question. C is the answer

Question #32

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.
Which configuration should the solutions architect choose to meet these requirements?

A. Configure Amazon CloudFront with AWS WAF.
B. Configure Application Load Balancers with AWS WAF.
C. Configure Amazon Route 53 with a geolocation policy.
D. Configure Amazon Route 53 with a geoproximity routing policy.

Commented [LC37]: With geolocation policy you can decide the content to distribute by country

Question #33

A solutions architect has created a new AWS account and must secure AWS account root user access.
Which combination of actions will accomplish this? (Choose two.)

A. Ensure the root user uses a strong password.
B. Enable multi-factor authentication to the root user.
C. Store root user access keys in an encrypted Amazon S3 bucket.
D. Add the root user to a group containing administrative permissions.
E. Apply the required permissions to the root user with an inline policy document.

Commented [LC38]: ANSWER

Question #34

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class.
Which S3 storage class should be implemented to meet these requirements?

A. S3 Glacier
B. S3 Intelligent-Tiering
C. S3 Standard-Infrequent Access (S3 Standard-IA)
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Commented [LC39]: ANSWER

Question #35

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution, and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.
What should a solutions architect do to protect the application?

A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Commented [LC40]: ANSWER

Question #36

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received.
How should the solutions architect integrate these components?

A. Use Amazon SQS FIFO queues.
B. Use an AWS Lambda function along with Amazon SQS standard queues.
C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Commented [LC41]: ANSWER

Question #37

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.
What should a solutions architect do to remediate the vulnerability?

A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

Commented [LC42]: Correct. You can't attach WAF to a NLB so B is wrong. A is never suggested. D is wrong because Shield is for DDOS attacks

Question #38

A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage. There are other internal systems that query this DB instance to fetch data for internal batch processing. The RDS DB instance slows down significantly when the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times.
Which solution will improve the website's performance?

A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
B. Use Amazon ElastiCache to cache the query responses for the website.
C. Add an additional Availability Zone to the current RDS MySQL Multi-AZ DB instance.
D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Commented [LC43]: A,C clearly wrong. B is wrong because the question doesn't mention common data so a cache may be useless. D is the most viable path.

Question #39

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.
What should a solutions architect do to maintain the desired performance across all instances in the group?

A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
B. Use a target tracking policy to dynamically scale the Auto Scaling group.
C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Commented [LC44]: Typical use for B

Ref: Configure a target tracking scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html

Question #40

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.
How should the scaling be changed to address the staff complaints and keep costs to a minimum?

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Commented [LC45]: Simple Scaling - There is a cool down period after the scaling activity. Meaning ASG has to wait for cooldown period to expire before responding to additional alarms. If you need a quick reaction time for scaling due to spike in load then this option might not be ideal.

Step Scaling - Since the scaling policy does not have "cool-down" period it can quickly scale up and respond to additional alarms even after scaling activity. It has however a "warm-up" period which is the time taken for instance to warm up. Until its specified warm-up time has expired, an instance is not counted toward the aggregated metrics of the Auto Scaling group. Good option if you quickly want to react to traffic load or traffic is unpredictable.

Target Tracking - Is a dynamic scaling policy which simplifies configuration and based on Cloudwatch metrics.

Answer is C

Question #41

A financial services company has a web application that serves users in the United States and Europe. The application consists of a database tier and a web server tier. The database tier consists of a MySQL database hosted in us-east-1. Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region. A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States.
Which changes should be made to the database tier to improve performance?

A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
B. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions.
C. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.
D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

Commented [LC46]: ANSWER

Question #42

A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost-effective solution.
What should a solutions architect do to accomplish this?

A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.
B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.
C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.
D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

Commented [LC47]: ANSWER

Question #43

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.
Which storage option would be the optimal solution?

A. Amazon Elastic File System (Amazon EFS)
B. Amazon FSx for Lustre
C. Amazon EC2 instance store
D. Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1)

Commented [LC48]: ANSWER

Question #44

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was install recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff.
What should the solutions architect recommend?

A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.
B. Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory.
C. Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance's security group to deny public access to Active Directory.

Commented [LC49]: Since it's a recommendation on the new design, I would answer A.

Question #45

A company hosts a static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.
Which action will accomplish this?

A. Enable Amazon S3 versioning.
B. Enable Amazon S3 Intelligent-Tiering.
C. Enable an Amazon S3 lifecycle policy.
D. Enable Amazon S3 cross-Region replication.

Commented [LC50]: ANSWER

Question #46

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application.
How can this be achieved?

A. Create hourly snapshots of the production RDS DB instance.
B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.
C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Commented [LC51]: ANSWER

Question #47

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.
Which solution meets these requirements?

A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Commented [LC52]: https://aws.amazon.com/it/storagegateway/hardware-appliance/

Question #48

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon Elastic Block Store (Amazon EBS) volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID).
What should a solutions architect do to meet these requirements?

A. Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance.
B. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon Elastic File System (Amazon EFS) and mount a target on each instance.
D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Commented [LC53]: Referring to https://cloudonaut.io/versus/storage/instance-store-vs-efs/

EFS is more resilient.

Question #49

A security team to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations.
The solution must be scalable and there must be a single point where permissions can be maintained.
What should a solutions architect do to accomplish this?

A. Create an ACL to provide access to the services or actions.
B. Create a security group to allow accounts and attach it to user groups.
C. Create cross-account roles in each account to deny access to the services or actions.
D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Commented [LC54]: ANSWER

Question #50

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only.
What is the MOST cost-effective solution?

A. Amazon S3 Glacier
B. Amazon S3 Standard
C. Amazon S3 Intelligent-Tiering
D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Commented [LC55]: A is for backups, D for infrequent access, C for unpredictable behaviours.

Question #51

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon Elastic Block Store (Amazon EBS) volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.
What should a solutions architect propose to ensure users see all of their documents at once?

A. Copy the data so both EBS volumes contain all the documents.
B. Configure the Application Load Balancer to direct a user to the server with the documents.
C. Copy the data from both EBS volumes to Amazon Elastic File System (Amazon EFS). Modify the application to save new documents to Amazon Elastic File System (Amazon EFS).
D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Commented [LC56]: ANSWER

Question #52

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.
What should a solutions architect use to accomplish this?

A. Server-Side Encryption with keys stored in an S3 bucket
B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Commented [LC57]: ANSWER

Question #53

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.
Which solution should be used to minimize costs?

A. Purchase Reserved Instances to cover 250 instances.
B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Commented [LC58]: ANSWER

Question #54

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.
Which combination of architectural changes will reduce the NAT gateway costs? (Choose two.)

A. Configure a VPC peering connection between the two VPCs. Access the API using the private address.
B. Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address.
C. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.
D. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address.
E. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.

Commented [LC59]: Starting May 1st 2021, all data transfer over a VPC Peering connection that stays within an Availability Zone (AZ) is now free. All data transfer over a VPC Peering connection that crosses Availability Zones will continue to be charged at the standard in-region data transfer rates. You can use the Availability Zone-ID to uniquely and consistently identify an Availability Zone across different AWS accounts.

Customers use VPC Peering to inter-connect VPCs within a region. VPC Peering is commonly used when interconnecting a small number of VPCs in a region to achieve full mesh connectivity. AWS Transit Gateway and AWS PrivateLink are the recommended mechanisms to inter-connect hundreds or thousands of VPCs at scale.

Commented [LC60]: AWS Resource Access Manager (RAM) helps you securely share your resources across AWS accounts, within your organization or organizational units (OUs) in AWS Organizations, and with IAM roles and IAM users for supported resource types. You can use AWS RAM to share transit gateways, subnets, AWS License Manager license configurations, Amazon Route 53 Resolver rules, and more resource types.

Question #55

A solutions architect is tasked with transferring 750 TB of data from an on-premises network-attached file system located at a branch office Amazon S3 Glacier.
The migration must not saturate the on-premises 1 Mbps internet connection.
Which solution will meet these requirements?

A. Create an AWS site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Transfer the files directly by using the AWS CLI.
B. Order 10 AWS Snowball Edge Storage Optimized devices, and select an S3 Glacier vault as the destination.
C. Mount the network-attached file system to an S3 bucket, and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
D. Order 10 AWS Snowball Edge Storage Optimized devices, and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

Commented [LC61]: You must go over S3 first.

Question #56

A company has a two-tier application architecture that runs in public and private subnets. Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet. The web application instances and the database are running in a single Availability Zone (AZ).
Which combination of steps should a solutions architect take to provide high availability for this architecture? (Choose two.)

A. Create new public and private subnets in the same AZ for high availability.
B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs.
C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer.
D. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ.
E. Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment.

Commented [LC62]: ANSWER

Commented [LC63]: ANSWER

Question #57

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent an accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.
Which combination of actions should be taken to meet these requirements? (Choose two.)

A. Enable a read-only bucket ACL.
B. Enable versioning on the bucket.
C. Attach an IAM policy to the bucket.
D. Enable MFA Delete on the bucket.
E. Encrypt the bucket using AWS KMS.

Commented [LC64]: ANSWER

Commented [LC65]: ANSWER

Question #58

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time.
What is the MOST secure way to do this?

A. Enable public read on the S3 object and provide the link to the vendor.
B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
C. Generate a presigned URL and have the vendor download the log file before it expires.
D. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.

Commented [LC66]: ANSWER

Question #59

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.
How should security groups be configured in this situation? (Choose two.)

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Commented [LC67]: ANSWER

Commented [LC68]: ANSWER

Question #60

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.
How should a solutions architect address this issue?

A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.
B. Use service control policies to disable IAM activity across all account in the organizational unit.
C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.
D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

Commented [LC69]: ANSWER

Question #61

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.
Which architecture should the solutions architect choose that provides high availability?

A. Create an Auto Scaling group that uses three instances across each of two Regions.
B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Commented [LC70]: ANSWER

Question #62

A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years.
The log files will be analysed by a reporting tool that must access all files concurrently.
Which storage solution meets these requirements MOST cost-effectively?

A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon EC2 instance store
D. Amazon S3

Commented [LC71]: ANSWER

Question #63

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.
Which database should a solutions architect recommend?

A. Amazon RDS for MySQL
B. Amazon RDS for PostgreSQL.
C. Amazon ElastiCache for Redis
D. Amazon ElastiCache for Memcached

Commented [LC72]: ANSWER

Ref: https://aws.amazon.com/it/elasticache/redis-vs-memcached/

Question #64

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website.
What should a solutions architect do to meet these requirements?

A. Redesign the application to use Amazon CloudFront.
B. Redesign the application to use AWS Elastic Beanstalk.
C. Redesign the application to use a Network Load Balancer.
D. Redesign the application to use Amazon S3 static website hosting.

Commented [LC73]: ANSWER

Question #65

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.
Which design should the solutions architect use?

A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Commented [LC74]: ANSWER

Question #66

A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.
Which action will MOST securely grant the EC2 instance access to the S3 bucket?

A. Attach a resource-based policy to the S3 bucket.
B. Create an IAM user for the application with specific permissions to the S3 bucket.
C. Associate an IAM role with least privilege permissions to the EC2 instance profile.
D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls.

Commented [LC75]: ANSWER

Question #67

A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow.
Which solution meets these requirements?

A. Use a database in Amazon RDS with Multi-AZ and at least one read replica.
B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica.
C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions.
D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones.

Commented [LC76]: ANSWER

Question #68

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.
Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling EC2_INSTANCE_LAUNCH events.

Commented [LC77]: ANSWER

Question #69

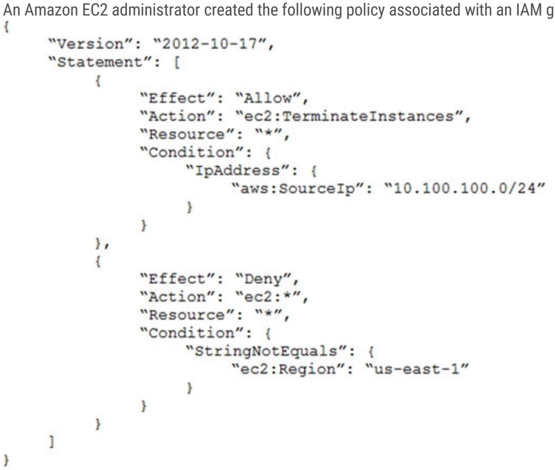
A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes for an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.
What should a solutions architect do to ensure messages are being processed once only?

A. Use the CreateQueue API call to create a new queue.
B. Use the AddPermission API call to add appropriate permissions.
C. Use the ReceiveMessage API call to set an appropriate wait time.
D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Commented [LC78]: Ref. https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html

Question #70

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:



```
{
     “Version”: “2012-10-17”,
     “Statement”: [
          {
               “Effect”: “Allow”,
               “Action”: “ec2:TerminateInstances”,
               “Resource”: “*”,
               “Condition”: {
                    “IpAddress”: {
                         “aws:SourceIp”: “10.100.100.0/24”
                    }
               }
          },
          {
               “Effect”: “Deny”,
               “Action”: “ec2:*”,
               “Resource”: “*”,
               “Condition”: {
                    “StringNotEquals”: {
                         “ec2:Region”: “us-east-1”
                    }
               }
          }
     ]
}
```

What is the effect of this policy?

A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
C. Users can terminate an EC2 instance in the us-east-1 Region when the user’s source IP is 10.100.100.254.
D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user’s source IP is 10.100.100.254.

Commented [LC79]: This one is a little tricky.
The condition StringNOTequals means it’s denying when it’s NOT us-east-1 ec2:* actions.
This means actions are not denied outside us-east-1.

So... Users can terminate an EC2 instance if they’re in us-east-1 and they have a source-ip 10.100.100.0/24

Answer is C.

B is wrong because the IP of the instance doesn’t have to be necessarily 10.100.100.0/24

Question #71

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.
Which service will improve the performance of both the real-time and on-demand steaming?

A. Amazon CloudFront
B. AWS Global Accelerator
C. Amazon Route S3
D. Amazon S3 Transfer Acceleration

Commented [LC80]: ANSWER

Question #72

A company has a three-tier image-sharing application. It uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application
Which solution meets these requirements?

A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users’ images.
B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users’ images.
C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users’ images.
D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users’ images.

Commented [LC81]: Answer is D. A is out because the website is not defined as a static. B is wrong because you don’t store images in RDS. C false as well because you don’t use the DB in a EC2 instance.

Question #73

A solutions architect is designing a system to analyse the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.
Which type of Amazon EC2 instances should be used to reduce the cost of the system?

A. Spot Instances
B. On-Demand Instances
C. Standard Reserved Instances
D. Scheduled Reserved Instances

Commented [LC82]: D is out because it’s not available anymore. C is tempting because of the “minimum of 1 year”. Although, I think the answer is B since the instances needs to be used only 4 hours every night, so it’s pointless to rent 1 year of instances that won’t be used for most of the time.

Question #74

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.
What should a solutions architect do to decouple the architecture and make it scalable?

A. Use Amazon S3 to serve the front-end application, which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic, and process and store the data in Amazon RDS.
C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.
D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway, which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.

Commented [LC83]: ANSWER

Question #75

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance.
Which storage option should the solutions architect recommend?

A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.

Commented [LC84]: ANSWER

C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon Elastic File System (Amazon EFS).
D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon Elastic Block Store (Amazon EBS).

Question #76

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.
Which action meets these requirements for storing and retrieving location data?

A. Use Amazon Athena with Amazon S3.
B. Use Amazon API Gateway with AWS Lambda.

Commented [LC85]: (Unsure between B and A) I'd pick B. Lambda looks more scalable and more able to deal with peak operating hours.

C. Use Amazon QuickSight with Amazon Redshift.
D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Question #77

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.
What should the solutions architect recommend?

A. Leverage Amazon CloudFront with the ALB endpoint as the origin.
B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB.

Commented [LC86]: WAS is a firewall service made for this purpose. Shield Advanced (and Shield) are for DDOS attacks.

C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked.
D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances.

Question #78

A company has an application that calls AWS Lambda functions. A code review shows that database credentials are stored in a Lambda function's source code, which violates the company's security policy. The credentials must be securely stored and must be automatically rotated on an ongoing basis to meet security policy requirements.
What should a solutions architect recommend to meet these requirements in the MOST secure manner?

A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can use the key ID to retrieve the password from CloudHSM. Use CloudHSM to automatically rotate the password.
B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can use the secret ID to retrieve the password from Secrets Manager. Use Secrets Manager to automatically rotate the password.

Commented [LC87]: ANSWER

C. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can use the key ID to retrieve the password from AWS KMS. Use AWS KMS to automatically rotate the uploaded password.
D. Move the database password to an environment variable that is associated with the Lambda function. Retrieve the password from the environment variable by invoking the function. Create a deployment script to automatically rotate the password.

Question #79

A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records.
Which services can the solutions architect recommend to meet these requirements?

A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

Commented [LC88]: ANSWER

Question #80

A company wants to use Amazon S3 for the secondary copy of its on-premises dataset. The company would rarely need to access this copy. The storage solution's cost should be minimal.
Which storage solution meets these requirements?

A. S3 Standard
B. S3 Intelligent-Tiering
C. S3 Standard-Infrequent Access (S3 Standard-IA)
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Commented [LC89]: ANSWER

Question #81

A company's operations team has an existing Amazon S3 bucket configured to notify an Amazon SQS queue when new objects are created within the bucket. The development team also wants to receive events when new objects are created. The existing operations team workflow must remain intact.
Which solution would satisfy these requirements?

A. Create another SQS queue. Update the S3 events in the bucket to also update the new queue when a new object is created.
B. Create a new SQS queue that only allows Amazon S3 to access the queue. Update Amazon S3 to update this queue when a new object is created.
C. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.
D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Add subscriptions for both queues in the topic.

Commented [LC90]: ANSWER

Question #82

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

A. Use a VPC endpoint for DynamoDB.
B. Use a NAT gateway in a public subnet.
C. Use a NAT instance in a private subnet.
D. Use the internet gateway attached to the VPC.

Commented [LC91]: ANSWER

Question #83

A company built an application that lets users check in to places they visit, rank the places, and add reviews about their experiences. The application is successful with a rapid increase in the number of users every month.
The chief technology officer fears the database supporting the current Infrastructure may not handle the new load the following month because the single Amazon RDS for MySQL instance has triggered alarms related to resource exhaustion due to read requests.
What can a solutions architect recommend to prevent service Interruptions at the database layer with minimal changes to code?

A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints. Enable a Multi-AZ deployment.
B. Create an Amazon EMR cluster and migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.
C. Create an Amazon ElastiCache cluster and redirect all read-only traffic to the cluster. Set up the cluster to be deployed in three Availability Zones.
D. Create an Amazon DynamoDB table to replace the RDS instance and redirect all read-only traffic to the DynamoDB table. Enable DynamoDB Accelerator to offload traffic from the main table.

Commented [LC92]: ANSWER

Question #84

A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.
What is the MOST cost-effective solution?

A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Commented [LC93]: ANSWER

Question #85

A company has created a VPC with multiple private subnets in multiple Availability Zones (AZs) and one public subnet in one of the AZs. The public subnet is used to launch a NAT gateway. There are instances in the private subnets that use a NAT gateway to connect to the internet. In case of an AZ failure, the company wants to ensure that the instances are not all experiencing internet connectivity issues and that there is a backup plan ready.
Which solution should a solutions architect recommend that is MOST highly available?

A. Create a new public subnet with a NAT gateway in the same AZ. Distribute the traffic between the two NAT gateways.
B. Create an Amazon EC2 NAT instance in a new public subnet. Distribute the traffic between the NAT gateway and the NAT instance.
C. Create public subnets in each AZ and launch a NAT gateway in each subnet. Configure the traffic from the private subnets in each AZ to the respective NAT gateway.
D. Create an Amazon EC2 NAT instance in the same public subnet. Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

Commented [LC94]: ANSWER

Question #86

A healthcare company stores highly sensitive patient records. Compliance requires that multiple copies be stored in different locations. Each record must be stored for 7 years. The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter.
What should a solutions architect recommend?

A. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy.
B. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier using a lifecycle policy.
C. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.
D. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.

Commented [LC95]: Deep Archive requires 12+ hours
Glacier requires between minutes (expedited) and 6 hours (standard)

Question #87

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.
Which solution achieves these goals MOST efficiently?

A. Use a scheduled AWS Lambda function and execute a script remotely on all EC2 instances to send data to the audit system.
B. Use EC2 Auto Scaling lifecycle hooks to execute a custom script to send data to the audit system when instances are launched and terminated.
C. Use an EC2 Auto Scaling launch configuration to execute a custom script through user data to send data to the audit system when instances are launched and terminated.
D. Execute a custom script on the instance operating system to send data to the audit system. Configure the script to be executed by the EC2 Auto Scaling group when the instance starts and is terminated.

Commented [LC96]: Ref: https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html

Question #88

A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.
Which solution should a solutions architect recommend to keep the data private?

A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.
B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.
C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in- time snapshots to AWS.
D. Deploy an AWS Storage Gateway file gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

Commented [LC97]: Unsure of this.

Question #89

A company has 150 TB of archived image data stored on-premises that needs to be moved to the AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only.
What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

A. Use AWS Snowmobile to ship the data to AWS.
B. Order multiple AWS Snowball devices to ship the data to AWS.
C. Enable Amazon S3 Transfer Acceleration and securely upload the data.
D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

Commented [LC98]: ANSWER

Question #90

A public-facing web application queries a database hosted on an Amazon EC2 instance in a private subnet. A large number of queries involve multiple table joins, and the application performance has been degrading due to an increase in complex queries. The application team will be performing updates to improve performance.
What should a solutions architect recommend to the application team? (Choose two.)

A. Cache query data in Amazon SQS
B. Create a read replica to offload queries
C. Migrate the database to Amazon Athena
D. Implement Amazon DynamoDB Accelerator to cache data.
E. Migrate the database to Amazon RDS

Commented [LC99]: ANSWER

Commented [LC100]: Tempted to pick C instead of B, Athena is not a database but a query engine, so wrong.

Question #91

A company is seeing access requests by some suspicious IP addresses. The security team discovers the requests are from different IP addresses under the same CIDR range.
What should a solutions architect recommend to the team?

A. Add a rule in the inbound table of the security to deny the traffic from that CIDR range.
B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.
C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.
D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

Commented [LC101]: ANSWER

Question #92

A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deployed on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. The company needs the ability shift traffic from resources in one region to another.
What should a solutions architect recommend?

A. Configure an Amazon Route 53 latency routing policy.
B. Configure an Amazon Route 53 geolocation routing policy.
C. Configure an Amazon Route 53 geoproximity routing policy.
D. Configure an Amazon Route 53 multivalue answer routing policy.

Commented [LC102]: Since it says “the company needs the ability to shift traffic from resources in one region to another” I’d pick C

Question #93

A company wants to replicate its data to AWS to recover in the event of a disaster. Today, a system administrator has scripts that copy data to a NFS share.
Individual backup files need to be accessed with low latency by application administrators to deal with errors in processing.
What should a solutions architect recommend to meet these requirements?

A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share.
B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share.
C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share.
D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

Commented [LC103]: ANSWER

Question #94

An application requires a development environment (DEV) and production environment (PROD) for several years. The DEV instances will run for 10 hours each day during normal business hours, while the PROD instances will run 24 hours each day. A solutions architect needs to determine a compute instance purchase strategy to minimize costs.
Which solution is the MOST cost-effective?

A. DEV with Spot Instances and PROD with On-Demand Instances
B. DEV with On-Demand Instances and PROD with Spot Instances
C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances
D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

Commented [LC104]: This answer is wrong now. Now the correct answer would be to use on-demand for DEV and reserved for PROD

Question #95

A company runs multiple Amazon EC2 Linux instances in a VPC with applications that use a hierarchical directory structure. The applications need to rapidly and concurrently read and write to shared storage.
How can this be achieved?

A. Create an Amazon Elastic File System (Amazon EFS) file system and mount it from each EC2 instance.
B. Create an Amazon S3 bucket and permit access from all the EC2 instances in the VPC.
C. Create a file system on an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volume. Attach the volume to all the EC2 instances.
D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes attached to each EC2 instance. Synchronize the Amazon Elastic Block Store (Amazon EBS) volumes across the different EC2 instances.

Commented [LC105]: ANSWER

Question #96

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.
What should the solutions architect do to meet these requirements?

A. Increase the minimum capacity for the Auto Scaling group.
B. Increase the maximum capacity for the Auto Scaling group.
C. Configure scheduled scaling to scale up to the desired compute level.
D. Change the scaling policy to add more EC2 instances during each scaling operation.

Commented [LC106]: ANSWER

Question #97

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access.
Which of the following would be the LEAST complicated implementation?

A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Commented [LC107]: ANSWER

Question #98

A solutions architect is designing a mission-critical web application. It will consist of Amazon EC2 instances behind an Application Load Balancer and a relational database. The database should be highly available and fault tolerant.
Which database implementations will meet these requirements? (Choose two.)

A. Amazon Redshift
B. Amazon DynamoDB
C. Amazon RDS for MySQL
D. MySQL-compatible Amazon Aurora Multi-AZ
E. Amazon RDS for SQL Server Standard Edition Multi-AZ

Commented [LC108]: ANSWER

Question #99

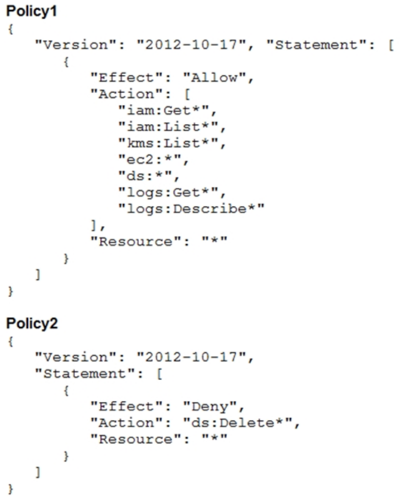
A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.
Which configuration will meet this requirement?

A. Configure the security group for the EC2 instances.
B. Configure the security group on the Application Load Balancer.
C. Configure AWS WAF on the Application Load Balancer in a VPC.
D. Configure the network ACL for the subnet that contains the EC2 instances.

Commented [LC109]: ANSWER

Question #100

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.



Policy1

```
{
   "Version": "2012-10-17", "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "iam:Get*",
            "iam:List*",
            "kms:List*",
            "ec2:*",
            "ds:*",
            "logs:Get*",
            "logs:Describe*"
         ],
         "Resource": "*"
      }
   ]
}
```

Policy2

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": "ds:Delete*",
         "Resource": "*"
      }
   ]
}
```

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

A. Deleting IAM users
B. Deleting directories
C. Deleting Amazon EC2 instances
D. Deleting logs from Amazon CloudWatch Logs

Commented [LC110]: ANSWER

Questions from 101-200

Question #101

A company has an Amazon EC2 instance running on a private subnet that needs to access a public website to download patches and updates. The company does not want external websites to see the EC2 instance IP address or initiate connections to it.
How can a solutions architect achieve this objective?

A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed.
B. Create a NAT gateway in a public subnet. Route outbound traffic from the private subnet through the NAT gateway.
C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website.
D. Create a security group that only allows connections from the IP address range of the public website. Attach the security group to the EC2 instance.

Commented [LC111]: ANSWER

Question #102

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

A. Use AWS Snowball.
B. Use AWS DataSync.
C. Use a secure VPN connection.
D. Use Amazon S3 Transfer Acceleration.

Commented [LC112]: ANSWER

Question #103

A company has a website running on Amazon EC2 instances across two Availability Zones. The company is expecting spikes in traffic on specific holidays, and wants to provide a consistent user experience. How can a solutions architect meet this requirement?

A. Use step scaling.
B. Use simple scaling.
C. Use lifecycle hooks.
D. Use scheduled scaling.

Commented [LC113]: ANSWER

Question #104

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.
Which action should be taken to improve the performance of the backend?

A. Implement Amazon SNS to store the database calls.
B. Implement Amazon ElastiCache to cache the large datasets.
C. Implement an RDS for MySQL read replica to cache database calls.
D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Commented [LC114]: “frequent calls” means caching, hence the answer.

Question #105

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.
How can these requirements be met?

A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.
B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.
D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

Commented [LC115]: ANSWER

Question #106

A company is processing data on a daily basis. The results of the operations are stored in an Amazon S3 bucket, analysed daily for one week, and then must remain immediately accessible for occasional analysis.
What is the MOST cost-effective storage solution alternative to the current configuration?

A. Configure a lifecycle policy to delete the objects after 30 days.
B. Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.
C. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Commented [LC116]: ANSWER

Question #107

A company delivers files in Amazon S3 to certain users who do not have AWS credentials. These users must be given access for a limited time.
What should a solutions architect do to securely meet these requirements?

A. Enable public access on an Amazon S3 bucket.
B. Generate a presigned URL to share with the users.
C. Encrypt files using AWS KMS and provide keys to the users.
D. Create and assign IAM roles that will grant GetObject permissions to the users.

Commented [LC117]: ANSWER

Question #108

A company wants to run a hybrid workload for data processing. The data needs to be accessed by on-premises applications for local data processing using an NFS protocol, and must also be accessible from the AWS Cloud for further analytics and batch processing.
Which solution will meet these requirements?

A. Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.
B. Use an AWS Storage Gateway tape gateway to copy the backup of the local data to AWS, then perform analytics on this data in the AWS cloud.
C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.
D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS cloud, then perform analytics on this data in the cloud.

Commented [LC118]: ANSWER

Question #109

A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandate encryption of data before sending it to Amazon S3.
What should a solutions architect recommend to satisfy these requirements?

A. Server-side encryption with customer-provided encryption keys
B. Client-side encryption with Amazon S3 managed encryption keys
C. Server-side encryption with keys stored in AWS key Management Service (AWS KMS)
D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

Commented [LC119]: ANSWER

Question #110

A solutions architect is moving the static content from a public website hosted on Amazon EC2 instances to an Amazon S3 bucket. An Amazon CloudFront distribution will be used to deliver the static assets. The security group used by the EC2 instances restricts access to a limited set of IP ranges. Access to the static content should be similarly restricted.
Which combination of steps will meet these requirements? (Choose two.)

A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.
C. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the CloudFront distribution.
D. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the S3 bucket hosting the static content.
E. Create a new IAM role and associate the role with the distribution. Change the permissions either on the S3 bucket or on the files within the S3 bucket so that only the newly created IAM role has read and download permissions.

Commented [LC120]: ANSWER

Question #111

A company is investigating potential solutions that would collect, process, and store users' service usage data. The business objective is to create an analytics capability that will enable the company to gather operational insights quickly using standard SQL queries. The solution should be highly available and ensure Atomicity, Consistency, Isolation, and Durability (ACID) compliance in the data tier.
Which solution should a solutions architect recommend?

A. Use an Amazon Timestream database.
B. Use an Amazon Neptune database in a Multi-AZ design.
C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design.
D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS) Throughput Optimized HDD (st1) storage.

Commented [LC121]: ANSWER

Question #112

A company recently launched its website to serve content to its global user base. The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin.
How should a solutions architect optimize high availability for the application?

A. Use Lambda@Edge for CloudFront.
B. Use Amazon S3 Transfer Acceleration for CloudFront.
C. Configure another EC2 instance in a different Availability Zone as part of the origin group.
D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

Commented [LC122]: ANSWER

Question #113

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both are in separate. AWS accounts. The network administrator needs to design a solution to enable secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.
Which solution will meet these requirements?

A. Set up a VPC peering connection between VPC-A and VPC-B.
B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
C. Attach a virtual private gateway to VPC-B and enable routing from VPC-A.
D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-B.

Commented [LC123]: A is the answer.

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

Question #114

A company currently stores symmetric encryption keys in a hardware security module (HSM). A solutions architect must design a solution to migrate key management to AWS. The solution should allow for key rotation and support the use of customer provided keys.
Where should the key material be stored to meet these requirements?

A. Amazon S3
B. AWS Secrets Manager
C. AWS Systems Manager Parameter store
D. AWS Key Management Service (AWS KMS)

Commented [LC124]: ANSWER

Question #115

A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.
What should a solutions architect recommend?

A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
B. Set up an Amazon Elastic File System (Amazon EFS) file system that connects with the backup applications using the NFS interface.
C. Set up an Amazon Elastic File System (Amazon EFS) file system that connects with the backup applications using the iSCSI interface.
D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Commented [LC125]: ANSWER

Question #116

A company hosts an application on an Amazon EC2 instance that requires a maximum of 200 GB storage space. The application is used infrequently, with peaks during mornings and evenings. Disk I/O varies, but peaks at 3,000 IOPS. The chief financial officer of the company is concerned about costs and has asked a solutions architect to recommend the most cost-effective storage option that does not sacrifice performance.
Which solution should the solutions architect recommend?

A. Amazon Elastic Block Store (Amazon EBS) Cold HDD (sc1)
B. Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2)
C. Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1)
D. Amazon Elastic Block Store (Amazon EBS) Throughput Optimized HDD (st1)

Commented [LC126]: B.

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

Question #117

A company's application hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Due to data sensitivity, traffic cannot traverse the internet.
How should a solutions architect configure access?

A. Create a private hosted zone using Amazon Route 53.
B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.
C. Configure AWS PrivateLink between the EC2 instance and the S3 bucket.
D. Set up a site-to-site VPN connection between the VPC and the S3 bucket.

Commented [LC127]: ANSWER

Question #118

A company has two applications it wants to migrate to AWS. Both applications process a large set of files by accessing the same files at the same time. Both applications need to read the files with low latency.
Which architecture should a solutions architect recommend for this situation?

A. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an instance store volume to store the data.
B. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume to store the data.
C. Configure one memory optimized Amazon EC2 instance to run both applications simultaneously. Create an Amazon Elastic Block Store (Amazon EBS) volume with Provisioned IOPS to store the data.
D. Configure two Amazon EC2 instances to run both applications. Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting Throughput mode to store the data.

Commented [LC128]: ANSWER

Question #119

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.
What should the solutions architect recommend?

A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
C. Create a read replica of the primary database and have the business analysts run their queries.
D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Commented [LC129]: ANSWER

Question #120

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest.
Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
B. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.
C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes.
D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

Commented [LC130]: This is the only one that encrypt the EBS volume as well.

Question #121

A company running an on-premises application is migrating the application to AWS to increase its elasticity and availability. The current architecture uses a Microsoft SQL Server database with heavy read activity. The company wants to explore alternate database options and migrate database engines, if needed.
Every 4 hours, the development team does a full copy of the production database to populate a test database. During this period, users experience latency.
What should a solutions architect recommend as replacement database?

A. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore from mysqldump for the test database.
B. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore snapshots from Amazon RDS for the test database.
C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas, and use the standby instance for the test database.
D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

Commented [LC131]: Here the assumption is that the DB was already converted in one of proposed in the answers.

So, let's take B as an example. B means there's a Aurora MultiAZ for production and from that, a test db must be populated. In order to do that, restoring the snapshot is the easiest thing.

C,D are out because of the engine. A is out because of the restoring method.

B is correct.

Question #122

A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts. The company has created a central AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users. The solution must be secure and optimized.
How should a solutions architect meet these requirements?

A. Configure an AWS Lambda function in each developer account to copy the log files to the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.
C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.

Commented [LC132]: ANSWER

Question #123

A company has several business systems that require access to data stored in a file share. The business systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company's legacy on-premises environments and with AWS.
Which services meet the business requirements? (Choose two.)

A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon FSx for Windows
D. Amazon S3
E. AWS Storage Gateway file gateway

Commented [LC133]: ANSWER

Commented [LC134]: ANSWER

Question #124

A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day. A solutions architect has been tasked with designing the MOST cost-effective solution.
Which solution will accomplish this?

A. Spot Fleet
B. Spot Instances
C. Reserved Instances
D. On-Demand Instances

Commented [LC135]: I'm not sure if it's A or D this time.

Which one is cheaper?

A Spot Fleet is set of Spot Instances and optionally On-Demand Instances that is launched based on criteria that you specify. The Spot Fleet selects the Spot capacity pools that meet your needs and launches Spot Instances to meet the target capacity for the fleet. By default, Spot Fleets are set to maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated. You can submit a Spot Fleet as a one-time request, which does not persist after the instances have been terminated. You can include On-Demand Instance requests in a Spot Fleet request.

B,C are out.

Question #125

A company has a Microsoft Windows-based application that must be migrated to AWS. This application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances.
What should a solutions architect do to accomplish this?

A. Configure a volume using Amazon Elastic File System (Amazon EFS). Mount the EFS volume to each Windows instance.
B. Configure AWS Storage Gateway in Volume Gateway mode. Mount the volume to each Windows instance.
C. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx volume to each Windows instance.
D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Commented [LC136]: ANSWER

Question #126

A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region.
What should a solutions architect do to automate the failover process?

A. Enable an ALB health check
B. Enable an Amazon Route 53 health check.
C. Create an CNAME record on Amazon Route 53 pointing to the ALB endpoint.
D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

Commented [LC137]: ANSWER

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html

Question #127

A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.
Which method should the solutions architect select?

A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Commented [LC138]: ANSWER

Question #128

A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However, the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds.
How can this issue be addressed?

A. Reduce the threshold for CPU utilization in the Auto Scaling group.
B. Replace the Application Load Balancer with a Network Load Balancer.
C. Add read replicas for the RDS instances and direct read traffic to the replica.
D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

Commented [LC139]: ANSWER

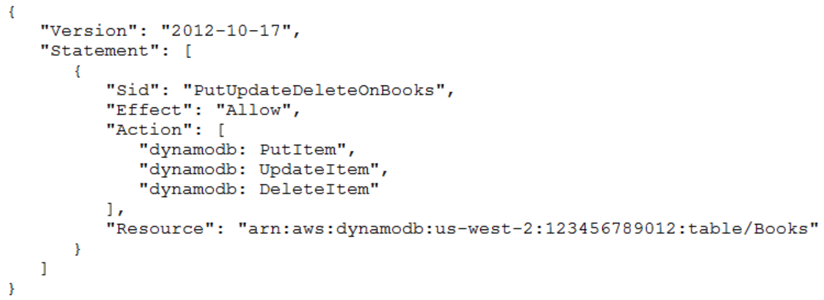
Question #129

A company has implemented one of its microservices on AWS Lambda that accesses an Amazon DynamoDB table named Books. A solutions architect is designing an IAM policy to be attached to the Lambda function's IAM role, giving it access to put, update, and delete items in the Books table. The IAM policy must prevent function from performing any other actions on the Books table or any other.

Which IAM policy would fulfil these needs and provide the LEAST privileged access?

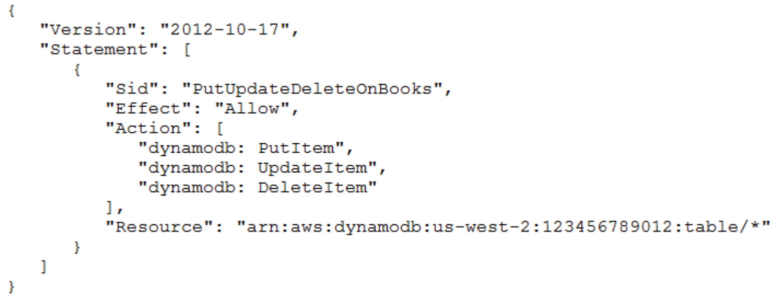
A.

Commented [LC140]: ANSWER



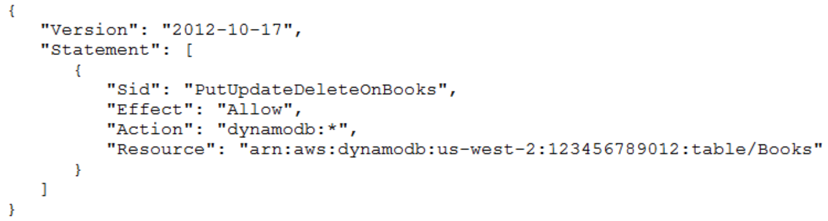
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Allow",
         "Action": [
            "dynamodb: PutItem",
            "dynamodb: UpdateItem",
            "dynamodb: DeleteItem"
         ],
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
      }
   ]
}
```

B.



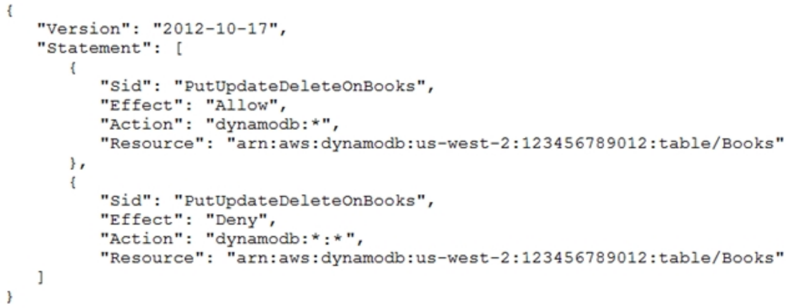
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Allow",
         "Action": [
            "dynamodb: PutItem",
            "dynamodb: UpdateItem",
            "dynamodb: DeleteItem"
         ],
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/*"
      }
   ]
}
```

C.



```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Allow",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
      }
   ]
}
```

D.



```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Allow",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
      },
      {
         "Sid": "PutUpdateDeleteOnBooks",
         "Effect": "Deny",
         "Action": "dynamodb:*:*",
         "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
   ]
}
```

Question #130

A company hosts its website on Amazon S3. The website serves petabytes of outbound traffic monthly, which accounts for most of the company's AWS costs.
What should a solutions architect do to reduce costs?

A. Configure Amazon CloudFront with the existing website as the origin.
B. Move the website to Amazon EC2 with Amazon Elastic Block Store (Amazon EBS) volumes for storage.
C. Use AWS Global Accelerator and specify the existing website as the endpoint.
D. Rearchitect the website to run on a combination of Amazon API Gateway and AWS Lambda.

Commented [LC141]: ANSWER

Question #131

A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer. Amazon Route 53 is used for the DNS. The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down.
How should the company deploy this solution?

A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.
B. Use Amazon S3 website hosting for the backup website and Route 53 latency routing policy.
C. Deploy the application in another AWS Region and use ELB health checks for failover routing.
D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

Commented [LC142]: ANSWER

Question #132

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.
Which set of services should a solutions architect recommend to meet these requirements?

A. Amazon Elastic Block Store (Amazon EBS) for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
B. Amazon Elastic Block Store (Amazon EBS) for maximum performance, Amazon Elastic File System (Amazon EFS) for durable data storage, and Amazon S3 Glacier for archival storage
C. Amazon EC2 instance store for maximum performance, Amazon Elastic File System (Amazon EFS) for durable data storage, and Amazon S3 for archival storage
D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Commented [LC143]: ANSWER

Question #133

A company uses Amazon S3 as its object storage solution. The company has thousands of S3 buckets it uses to store data. Some of the S3 buckets have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented or are implemented partially, resulting in data being stored in high-cost storage.
Which solution will lower costs without compromising the availability of objects?

A. Use S3 ACLs.
B. Use Amazon Elastic Block Store (Amazon EBS) automated snapshots.
C. Use S3 Intelligent-Tiering storage.
D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA).

Commented [LC144]: ANSWER

Question #134

An application is running on Amazon EC2 instances. Sensitive information required for the application is stored in an Amazon S3 bucket. The bucket needs to be protected from internet access while only allowing services within the VPC access to the bucket.
Which combination of actions should solutions archived take to accomplish this? (Choose two.)

A. Create a VPC endpoint for Amazon S3.
B. Enable server access logging on the bucket.
C. Apply a bucket policy to restrict access to the S3 endpoint.
D. Add an S3 ACL to the bucket that has sensitive information.
E. Restrict users using the IAM policy to use the specific bucket.

Commented [LC145]: ANSWER

Commented [LC146]: ANSWER

Question #135

A web application runs on Amazon EC2 instances behind an Application Load Balancer. The application allows users to create custom reports of historical weather data. Generating a report can take up to 5 minutes. These long-running requests use many of the available incoming connections, making the system unresponsive to other users.
How can a solutions architect make the system more responsive?

A. Use Amazon SQS with AWS Lambda to generate reports.
B. Increase the idle timeout on the Application Load Balancer to 5 minutes.
C. Update the client-side application code to increase its request timeout to 5 minutes.
D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading to the user.

Commented [LC147]: ANSWER

Question #136

A solutions architect must create a highly available bastion host architecture. The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain.
What should the solutions architect do to meet these requirements?

A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.
B. Create a Network Load Balancer backed by a Spot Fleet with instances in a partition placement group.
C. Create a Network Load Balancer backed by the existing servers in different Availability Zones as the target.
D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target.

Commented [LC148]: ANSWER

Question #137

A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS, and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times.
Which action will be MOST effective in accomplishing this?

A. Replace the SQS queue with Amazon Kinesis Data Firehose.
B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.
C. Add an Amazon CloudFront distribution to cache the responses for the web tier.
D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.

Commented [LC149]: ANSWER

Question #138

A company relies on an application that needs at least 4 Amazon EC2 instances during regular traffic and must scale up to 12 EC2 instances during peak loads.
The application is critical to the business and must be highly available.
Which solution will meet these requirements?

A. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with 2 in Availability Zone A and 2 in Availability Zone B.
B. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with all 4 in Availability Zone A.
C. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B.
D. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with all 8 in Availability Zone A.

Commented [LC150]: ANSWER

Question #139

A solutions architect must design a solution for a persistent database that is being migrated from on-premises to AWS. The database requires 64,000 IOPS according to the database administrator. If possible, the database administrator wants to use a single Amazon Elastic Block Store (Amazon EBS) volume to host the database instance.
Which solution effectively meets the database administrator's criteria?

A. Use an instance from the I3 I/O optimized family and leverage local ephemeral storage to achieve the IOPS requirement.
B. Create a Nitro-based Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.
C. Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.
D. Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

Commented [LC151]: ANSWER

Question #140

A solutions architect is designing an architecture for a new application that requires low network latency and high network throughput between Amazon EC2 instances. Which component should be included in the architectural design?

A. An Auto Scaling group with Spot Instance types.
B. A placement group using a cluster placement strategy.
C. A placement group using a partition placement strategy.
D. An Auto Scaling group with On-Demand instance types.

Commented [LC152]: ANSWER

Questions from 201-300

Question #211

A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.
What should the solutions architect do to reduce the overall data transfer costs?

A. Place all the EC2 instances in an Auto Scaling group.
B. Place all the EC2 instances in the same AWS Region.
C. Place all the EC2 instances in the same Availability Zone.
D. Place all the EC2 instances in private subnets in multiple Availability Zones.

Commented [LC153]: ANSWER

Question #212

A company hosts its core network services, including directory services and DNS, in its on-premises data center. The data center is connected to the AWS Cloud using AWS Direct Connect (DX). Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network services.
What should a solutions architect implement to meet these requirements with the LEAST amount of operational overhead?

A. Create a DX connection in each new account. Route the network traffic to the on-premises servers.
B. Configure VPC endpoints in the DX VPC for all required services. Route the network traffic to the on-premises servers.
C. Create a VPN connection between each new account and the DX VPC. Route the network traffic to the on-premises servers.
D. Configure AWS Transit Gateway between the accounts. Assign DX to the transit gateway and route network traffic to the on-premises servers.

Commented [LC154]: ANSWER

Question #213

A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.
What should a solutions architect recommend?

A. Deploy Amazon Inspector and associate it with the ALB.
B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Commented [LC155]: ANSWER

Question #214

A company receives structured and semi-structured data from various sources once every day. A solutions architect needs to design a solution that leverages big data processing frameworks. The data should be accessible using SQL queries and business intelligence tools.
What should the solutions architect recommend to build the MOST high-performing solution?

A. Use AWS Glue to process data and Amazon S3 to store data.
B. Use Amazon EMR to process data and Amazon Redshift to store data.
C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data.
D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data.

Commented [LC156]: ANSWER

Question #215

A company is hosting an election reporting website on AWS for users around the world. The website uses Amazon EC2 instances for the web and application tiers in an Auto Scaling group with Application Load Balancers. The database tier uses an Amazon RDS for MySQL database. The website is updated with election results once an hour and has historically observed hundreds of users accessing the reports.
The company is expecting a significant increase in demand because of upcoming elections in different countries. A solutions architect must improve the website's ability to handle additional demand while minimizing the need for additional EC2 instances.
Which solution will meet these requirements?

A. Launch an Amazon ElastiCache cluster to cache common database queries.
B. Launch an Amazon CloudFront web distribution to cache commonly requested website content.
C. Enable disk-based caching on the EC2 instances to cache commonly requested website content.
D. Deploy a reverse proxy into the design using an EC2 instance with caching enabled for commonly requested website content.

Commented [LC157]: ANSWER

Question #216

A company is building a website that relies on reading and writing to an Amazon DynamoDB database. The traffic associated with the website predictably peaks during business hours on weekdays and declines overnight and during weekends. A solutions architect needs to design a cost-effective solution that can handle the load.
What should the solutions architect do to meet these requirements?

A. Enable DynamoDB Accelerator (DAX) to cache the data.
B. Enable Multi-AZ replication for the DynamoDB database.

C. Enable DynamoDB auto scaling when creating the tables.
D. Enable DynamoDB On-Demand capacity allocation when creating the tables.

Commented [LC158]: This would be the ANSWER and not D because we aim to a cost effective solution. With C we are less flexible but at the same we save money still autoscaling the db.

Question #217

A company uses Amazon Redshift for its data warehouse. The company wants to ensure high durability for its data in case of any component failure.
What should a solutions architect recommend?

A. Enable concurrency scaling.
B. Enable cross-Region snapshots.
C. Increase the data retention period.
D. Deploy Amazon Redshift in Multi-AZ.

Commented [LC159]: Q: Does Amazon Redshift support Multi-AZ Deployments?

Currently, Amazon Redshift only supports Single-AZ deployments. You can run data warehouse clusters in multiple AZ's by loading data into two Amazon Redshift data warehouse clusters in separate AZs from the same set of Amazon S3 input files. With Redshift Spectrum, you can spin up multiple clusters across AZs and access data in Amazon S3 without having to load it into your cluster. In addition, you can also restore a data warehouse cluster to a different AZ from your data warehouse cluster snapshots.

Question #218

A company has data stored in an on-premises data center that is used by several on-premises applications. The company wants to maintain its existing application environment and be able to use AWS services for data analytics and future visualizations.
Which storage service should a solutions architect recommend?

A. Amazon Redshift
B. AWS Storage Gateway for files
C. Amazon Elastic Block Store (Amazon EBS)
D. Amazon Elastic File System (Amazon EFS)

Commented [LC160]: Key is "on-premise" data center

Question #219

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF.
How should the solutions architect comply with these requirements?

A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Commented [LC161]: ANSWER

Question #220

A company has a 143 TB MySQL database that it wants to migrate to AWS. The plan is to use Amazon Aurora MySQL as the platform going forward. The company has a 100 Mbps AWS Direct Connect connection to Amazon VPC.
Which solution meets the company's needs and takes the LEAST amount of time?

A. Use a gateway endpoint for Amazon S3. Migrate the data to Amazon S3. Import the data into Aurora.
B. Upgrade the Direct Connect link to 500 Mbps. Copy the data to Amazon S3. Import the data into Aurora.
C. Order an AWS Snowmobile and copy the database backup to it. Have AWS import the data into Amazon S3. Import the backup into Aurora.
D. Order four 50-TB AWS Snowball devices and copy the database backup onto them. Have AWS import the data into Amazon S3. Import the data into Aurora.

Commented [LC162]: At that speed-rate it's not feasible to migrate all that data, the snowball come handy for these purposes.

Question #221

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.
Which solution meets these requirements?

A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

Commented [LC163]: KISS rule always good in IT. The others are overcomplicating what could be easily done in few steps

Question #222

A company has a 10 Gbps AWS Direct Connect connection from its on-premises servers to AWS. The workloads using the connection are critical. The company requires a disaster recovery strategy with maximum resiliency that maintains the current connection bandwidth at a minimum.
What should a solutions architect recommend?

A. Set up a new Direct Connect connection in another AWS Region.
B. Set up a new AWS managed VPN connection in another AWS Region.
C. Set up two new Direct Connect connections: one in the current AWS Region and one in another Region.
D. Set up two new AWS managed VPN connections: one in the current AWS Region and one in another Region.

Commented [LC164]: A would be fine as well but since they're asking for Maximum Resiliency I'd pick C

Question #223

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.
What should the solutions architect do to enable internet access for the private subnets?

A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress- only internet gateway.

Commented [LC165]: Classic NAT Gateway usage

Question #224

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.
Which solution meets these requirements?

A. Run a query with Amazon Athena to generate the report.
B. Create a report in Cost Explorer and download the report.
C. Access the bill details from the billing dashboard and download the bill.
D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Commented [LC166]: ANSWER

Question #225

A company with facilities in North America, Europe, and Asia is designing new distributed application to optimize its global supply chain and manufacturing process. The orders booked on one continent should be visible to all Regions in a second or less. The database should be able to support failover with a short Recovery Time Objective (RTO). The uptime of the application is important to ensure that manufacturing is not impacted.
What should a solutions architect recommend?

A. Use Amazon DynamoDB global tables.
B. Use Amazon Aurora Global Database.
C. Use Amazon RDS for MySQL with a cross-Region read replica.
D. Use Amazon RDS for PostgreSQL with a cross-Region read replica.

Commented [LC167]: ANSWER

DynamoDB has no need for failover

Ref: https://www.capitalone.com/tech/software-engineering/comparing-dynamodb-and-aurora-global-database-and-aurora-multi-master/

Question #226

A company's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.
Which combination of steps should the solutions architect take? (Choose two.)

A. Use Amazon Kinesis Data Firehose to ingest the data.
B. Use AWS Lambda with AWS Step Functions to process the data.
C. Use AWS Database Migration Service (AWS DMS) to ingest the data.
D. Use Amazon EC2 instances in an Auto Scaling group to process the data.
E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Commented [LC168]: ANSWER

Commented [LC169]: ANSWER

Question #227

An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table. Both the EC2 instance and the DynamoDB table are in the same AWS account. A solutions architect must configure the necessary permissions.
Which solution will allow least privilege access to the DynamoDB table from the EC2 instance?

A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance.
B. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Add the EC2 instance to the trust relationship policy document to allow it to assume the role.
C. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Store the credentials in an Amazon S3 bucket and read them from within the application code directly.
D. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls.

Commented [LC170]: ANSWER

Question #228

A solutions architect is designing a solution that involves orchestrating a series of Amazon Elastic Container Service (Amazon ECS) task types running on Amazon EC2 instances that are part of an ECS cluster. The output and state data for all tasks needs to be stored. The amount of data output by each task is approximately 10 MB, and there could be hundreds of tasks running at a time. The system should be optimized for high-frequency reading and writing. As old outputs are archived and deleted, the storage size is not expected to exceed 1 TB.
Which storage solution should the solutions architect recommend?

A. An Amazon DynamoDB table accessible by all ECS cluster instances.
B. An Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.
C. An Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode.
D. An Amazon Elastic Block Store (Amazon EBS) volume mounted to the ECS cluster instances.

Commented [LC171]: Since the file system shouldn't exceed 1 TB, it means that B is enough. C works when the file system varies

Question #229

An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service: free and paid. Photos submitted by paid users are processed before those submitted by free users. Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS.
Which configuration should a solutions architect recommend?

A. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.
B. Use two SQS FIFO queues: one for paid and one for free. Set the free queue to use short polling and the paid queue to use long polling.
C. Use two SQS standard queues: one for paid and one for free. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.
D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero. Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first.

Commented [LC172]: ANSWER

Question #230

A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.
Which solution meets these requirements?

A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Commented [LC173]: ANSWER

Question #231

A company stores user data in AWS. The data is used continuously with peak usage during business hours. Access patterns vary, with some data not being used for months at a time. A solutions architect must choose a cost-effective solution that maintains the highest level of durability while maintaining high availability.
Which storage solution meets these requirements?

A. Amazon S3 Standard
B. Amazon S3 Intelligent-Tiering
C. Amazon S3 Glacier Deep Archive
D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Commented [LC174]: ANSWER

Question #232

A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failure environment on AWS in case the on-premises data center fails.
The company runs web servers that connect to external vendors. The data available on AWS and on premises must be uniform.
Which solution should a solutions architect recommend that has the LEAST amount of downtime?

A. Configure an Amazon Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
B. Configure an Amazon Route 53 failover record. Execute an AWS CloudFormation template from a script to create Amazon EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
C. Configure an Amazon Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on Amazon EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer.
D. Configure an Amazon Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two Amazon EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3. Set up an AWS Direct Connect connection between a VPC and the data center.

Commented [LC175]: ANSWER

Question #233

A company has three VPCs named Development, Testing, and Production in the us-east-1 Region. The three VPCs need to be connected to an on-premises data center and are designed to be separate to maintain security and prevent any resource sharing. A solutions architect needs to find a scalable and secure solution.
What should the solutions architect recommend?

A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.
B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.
C. Connect VPN connections from all the VPCs to a VPN in the Production VPC. Use a VPN connection from the Production VPC back to the data center.
D. Create a new VPC called Network. Within the Network VPC, create an AWS Transit Gateway with an AWS Direct Connect connection back to the data center. Attach all the other VPCs to the Network VPC.

Commented [LC176]: ANSWER

Question #234

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.
B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.
C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.
D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

Commented [LC177]: ANSWER

Question #235

A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly.
What is the MOST cost-effective method to establish this type of connection?

A. Implement a client VPN.
B. Implement AWS Direct Connect.
C. Implement a bastion host on Amazon EC2.
D. Implement an AWS Site-to-Site VPN connection.

Commented [LC178]: Direct Connect requires weeks to be available. A bastion host on EC2 is used for other purposes. A client VPN is not enough, D fulfills all objectives

Question #236

A company uses Application Load Balancers (ALBs) in different AWS Regions. The ALBs receive inconsistent traffic that can spike and drop throughout the year.
The company's networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.
Which solution is the MOST scalable with minimal configuration changes?

A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions. Update the on-premises firewall's rule to allow the IP addresses of the ALBs.
B. Migrate all ALBs in different Regions to the Network Load Balancer (NLBs). Update the on-premises firewall's rule to allow the Elastic IP addresses of all the NLBs.
C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall's rule to allow static IP addresses associated with the accelerator.
D. Launch a Network Load Balancer (NLB) in one Region. Register the private IP addresses of the ALBs in different Regions with the NLB. Update the on- premises firewall's rule to allow the Elastic IP address attached to the NLB.

Commented [LC179]: ANSWER

Question #237

A company runs a high performance computing (HPC) workload on AWS. The workload required low-latency network performance and high network throughput with tightly coupled node-to-node communication. The Amazon EC2 instances are properly sized for compute and storage capacity, and are launched using default options.
What should a solutions architect propose to improve the performance of the workload?

A. Choose a cluster placement group while launching Amazon EC2 instances.
B. Choose dedicated instance tenancy while launching Amazon EC2 instances.
C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances.
D. Choose the required capacity reservation while launching Amazon EC2 instances.

Commented [LC180]: ANSWER

Question #238

A company uses a legacy on-premises analytics application that operates on gigabytes of .csv files and represents months of data. The legacy application cannot handle the growing size of .csv files. New .csv files are added daily from various data sources to a central on-premises storage location. The company wants to continue to support the legacy application while users learn AWS analytics services. To achieve this, a solutions architect wants to maintain two synchronized copies of all the .csv files on-premises and in Amazon S3.
Which solution should the solutions architect recommend?

A. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between the company's on-premises storage and the company's S3 bucket.
B. Deploy an on-premises file gateway. Configure data sources to write the .csv files to the file gateway. Point the legacy analytics application to the file gateway. The file gateway should replicate the .csv files to Amazon S3.
C. Deploy an on-premises volume gateway. Configure data sources to write the .csv files to the volume gateway. Point the legacy analytics application to the volume gateway. The volume gateway should replicate data to Amazon S3.
D. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between on-premises and Amazon Elastic File System (Amazon EFS). Enable replication from Amazon Elastic File System (Amazon EFS) to the company's S3 bucket.

Commented [LC181]: Since they cannot handle the growing size, I'd say File Gateway, which is unlimited storage option that doesn't full the on-prem storage

Question #239

A company has media and application files that need to be shared internally. Users currently are authenticated using Active Directory and access files from a Microsoft Windows platform. The chief executive officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit.
What should a solutions architect recommend?

A. Set up a corporate Amazon S3 bucket and move all media and application files.
B. Configure Amazon FSx for Windows File Server and move all the media and application files.
C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.
D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes, and move all media and application files.

Commented [LC182]: FSx integrates with AD to provide a network drive inside a domain

Question #240

A company is deploying a web portal. The company wants to ensure that only the web portion of the application is publicly accessible. To accomplish this, the VPC was designed with two public subnets and two private subnets. The application will run on several Amazon EC2 instances in an Auto Scaling group. SSL termination must be offloaded from the EC2 instances.
What should a solutions architect do to ensure these requirements are met?

A. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
B. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the public subnets and associate it with the Application Load Balancer.
C. Configure the Application Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
D. Configure the Application Load Balancer in the private subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

Commented [LC183]: ANSWER

Question #241

A company is experiencing growth as demand for its product has increased. The company's existing purchasing application is slow when traffic spikes. The application is a monolithic three-tier application that uses synchronous transactions and sometimes sees bottlenecks in the application tier. A solutions architect needs to design a solution that can meet required application response times while accounting for traffic volume spikes.
Which solution will meet these requirements?

A. Vertically scale the application instance using a larger Amazon EC2 instance size.
B. Scale the application's persistence layer horizontally by introducing Oracle RAC on AWS.
C. Scale the web and application tiers horizontally using Auto Scaling groups and an Application Load Balancer.
D. Decouple the application and data tiers using Amazon Simple Queue Service (Amazon SQS) with asynchronous AWS Lambda calls.

Commented [LC184]: C. D doesn't convince me because it says that uses synchronous transactions while D proposes asynchronous lambda calls

Question #242

A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata, which takes less than 5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements.
What should the solutions architect recommend?

A. Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.
B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.
D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

Commented [LC185]: That's the standard usage for lambda, it's even indicated in the main use cases of the docs

Question #243

A company has copied 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region using an AWS Direct Connect link. The company now wants to copy the data to another S3 bucket in the us-west-2 Region. The colocation facility does not allow the use of AWS Snowball.
What should a solutions architect recommend to accomplish this?

A. Order a Snowball Edge device to copy the data from one Region to another Region.
B. Transfer contents from the source S3 bucket to a target S3 bucket using the S3 console.
C. Use the aws S3 sync command to copy data from the source bucket to the destination bucket.
D. Add a cross-Region replication configuration to copy objects across S3 buckets in different Regions.

Commented [LC186]: D is tempting but Cross Replication has a downside, it doesn't work for existing objects but only for new objects, this means that it's not a feasible path to do.

Hence, answer is C.

Question #244

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.
Which solution provides near-real-time data querying that is scalable with minimal data loss?

A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.
B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

Commented [LC187]: ANSWER

A is wrong because Data Streams doesn't scale automatically

Question #245

A company is deploying a multi-instance application within AWS that requires minimal latency between the instances.
What should a solutions architect recommend?

A. Use an Auto Scaling group with a cluster placement group.
B. Use an Auto Scaling group with single Availability Zone in the same AWS Region.
C. Use an Auto Scaling group with multiple Availability Zones in the same AWS Region.
D. Use a Network Load Balancer with multiple Amazon EC2 Dedicated Hosts as the targets.

Commented [LC188]: Cluster placement group is made for that purpose

Question #246

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.
What should the solutions architect do to meet these requirements?

A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Commented [LC189]: ANSWER

Question #247

A company is building a document storage application on AWS. The application runs on Amazon EC2 instances in multiple Availability Zones. The company requires the document store to be highly available. The documents need to be returned immediately when requested. The lead engineer has configured the application to use Amazon Elastic Block Store (Amazon EBS) to store the documents, but is willing to consider other options to meet the availability requirement.
What should a solutions architect recommend?

A. Snapshot the EBS volumes regularly and build new volumes using those snapshots in additional Availability Zones.
B. Use Amazon Elastic Block Store (Amazon EBS) for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3.
C. Use Amazon Elastic Block Store (Amazon EBS) for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3 Glacier.
D. Use at least three Provisioned IOPS EBS volumes for EC2 instances. Mount the volumes to the EC2 instances in a RAID 5 configuration.

Commented [LC190]: C can't be because of retrieval time. A is just not practical. D is not possible to do.

Question #248

A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Which statement should a solutions architect add to the policy to correct bucket access?

A.

```
"Action": [
    "s3:*Object"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

B.

```
"Action": [
    "s3:*"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

C.

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name*"
],
"Effect": "Allow"
```

D.

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

Commented [LC191]: ANSWER

Question #249

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
C. Create a service control policy (SCP) the prohibits changes to CloudTrail, and attach it the developer accounts.
D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account.

Commented [LC192]: ANSWER

Question #250

A company wants to share forensic accounting data that is stored in an Amazon RDS DB instance with an external auditor. The auditor has its own AWS account and requires its own copy of the database.
How should the company securely share the database with the auditor?

A. Create a read replica of the database and configure IAM standard database authentication to grant the auditor access.
B. Copy a snapshot of the database to Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket.
C. Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket.
D. Make an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

Commented [LC193]: ANSWER

Question #251

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.
Which design should a solutions architect recommend?

A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.
B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume.
C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.
D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

Commented [LC194]: ANSWER

Question #252

A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation.
The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses.
What should a solutions architect recommend to support this workload?

A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.
B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.
D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

Commented [LC195]: I am not completely sure about this but I would rather pick this than C because with C we have a maximum time of 15 minutes, which this job may exceed for its purposes.

Question #253

A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.
What should the solutions architect do to accomplish this?

A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Commented [LC196]: ANSWER

Question #254

An application is running on an Amazon EC2 instance and must have millisecond latency when running the workload. The application makes many small reads and writes to the file system, but the file system itself is small.
Which Amazon Elastic Block Store (Amazon EBS) volume type should a solutions architect attach to their EC2 instance?

A. Cold HDD (sc1)
B. General Purpose SSD (gp2)
C. Provisioned IOPS SSD (io1)
D. Throughput Optimized HDD (st1)

Commented [LC197]: ANSWER

Question #255

A solutions architect is designing a multi-Region disaster recovery solution for an application that will provide public API access. The application will use Amazon EC2 instances with a userdata script to load application code and an Amazon RDS for MySQL database. The Recovery Time Objective (RTO) is 3 hours and the Recovery Point Objective (RPO) is 24 hours.
Which architecture would meet these requirements at the LOWEST cost?

A. Use an Application Load Balancer for Region failover. Deploy new EC2 instances with the userdata script. Deploy separate RDS instances in each Region.
B. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script. Create a read replica of the RDS instance in a backup Region.
C. Use Amazon API Gateway for the public APIs and Region failover. Deploy new EC2 instances with the userdata script. Create a MySQL read replica of the RDS instance in a backup Region.
D. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script for APIs, and create a snapshot of the RDS instance daily for a backup. Replicate the snapshot to a backup Region.

Commented [LC198]: Since it asks for lowest cost, I'd say D. If it was asking for best solution, I'd say A

Question #256

A solutions architect needs to ensure that all Amazon Elastic Block Store (Amazon EBS) volumes restored from unencrypted EBC snapshots are encrypted.
What should the solutions architect do to accomplish this?

A. Enable EBS encryption by default for the AWS Region.
B. Enable EBS encryption by default for the specific volumes.
C. Create a new volume and specify the symmetric customer master key (CMK) to use for encryption.
D. Create a new volume and specify the asymmetric customer master key (CMK) to use for encryption.

Commented [LC199]: We need to ensure that ALL EBS volumes are encrypted. Hence, A

Question #257

A company runs a static website through its on-premises data center. The company has multiple servers that handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable. The company wants to expand its presence globally and plans to triple its website traffic.
What should a solutions architect recommend to meet these requirements?

A. Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.
B. Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.
C. Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.
D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

Commented [LC200]: It's a static website, so it's the best choice.

Question #258

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.
What should the solutions architect recommend?

A. Implement EC2 Spot Instances.
B. Purchase EC2 Reserved Instances.
C. Implement EC2 On-Demand Instances.
D. Implement the processing on AWS Lambda.

Commented [LC201]: Spot instances are the cheapest and can be interrupted with no warning. Here it's the best choice since it's a stateless processing

Question #259

A company is hosting its static website in an Amazon S3 bucket, which is the origin for Amazon CloudFront. The company has users in the United States, Canada, and Europe and wants to reduce costs.
What should a solutions architect recommend?

A. Adjust the CloudFront caching time to live (TTL) from the default to a longer timeframe.
B. Implement CloudFront events with Lambda@Edge to run the website's data processing.
C. Modify the CloudFront price class to include only the locations of the countries that are served.
D. Implement a CloudFront Secure Sockets Layer (SSL) certificate to push security closer to the locations of the countries that are served.

Commented [LC202]: ANSWER

Question #260

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.
Which Amazon EC2 pricing option is the MOST cost-effective?

A. Dedicated Reserved Hosts
B. Dedicated On-Demand Hosts
C. Dedicated Reserved Instances
D. Dedicated On-Demand Instances

Commented [LC203]: Reserved Hosts are hosts that allows you to bring your own licenses of your softwares (BYOL model)

Question #261

A company is designing a website that uses an Amazon S3 bucket to store static images. The company wants all future requests to have faster response times while reducing both latency and cost.
Which service configuration should a solutions architect recommend?

A. Deploy a NAT server in front of Amazon S3.
B. Deploy Amazon CloudFront in front of Amazon S3.
C. Deploy a Network Load Balancer in front of Amazon S3.
D. Configure Auto Scaling to automatically adjust the capacity of the website.

Commented [LC204]: That's CF purpose

Question #262

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.
Which service should a solutions architect recommend?

A. Amazon Aurora MySQL
B. Amazon Aurora Serverless for MySQL
C. Amazon Redshift Spectrum
D. Amazon RDS for MySQL

Commented [LC205]: ANSWER

Question #263

A company needs to comply with a regulatory requirement that states all emails must be stored and archived externally for 7 years. An administrator has created compressed email files on premises and wants a managed service to transfer the files to AWS storage.
Which managed service should a solutions architect recommend?

A. Amazon Elastic File System (Amazon EFS)
B. Amazon S3 Glacier
C. AWS Backup
D. AWS Storage Gateway

Commented [LC206]: Since it's on-prem, it's D

Question #264

A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named CompanyConfidential. The cloud engineer must be able to read from and write to an S3 bucket called AdminTools.
Which IAM policy will meet these requirements?

A.

Commented [LC207]: ANSWER

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::AdminTools"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

B.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::AdminTools",
                "arn:aws:s3:::CompanyConfidential/*"
                ]
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::CompanyConfidential"
        }
    ]
}
{
```

C.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*",
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

D.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential",
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::AdminTools/*"
            ]
        }
    ]
}
```

Question #265

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check.
What should a solutions architect do to accomplish this?

A. Use AWS Config rules to define and detect resources that are not properly tagged.
B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Commented [LC208]: B could be feasible as well, but we aim to minimise the effort, so A

Question #266

A company has a live chat application running on its on-premises servers that use WebSockets. The company wants to migrate the application to AWS. Application traffic is inconsistent, and the company expects there to be more traffic with sharp spikes in the future.
The company wants a highly scalable solution with no server maintenance nor advanced capacity planning.
Which solution meets these requirements?

A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.
B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
C. Run Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
D. Run Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.

Commented [LC209]: Serverless so C, D must be excluded. A would be good but provisioned capacity DynamoDB is not scalable. B takes care of that as well.

Question #267

A company hosts its static website content from an Amazon S3 bucket in the us-east-1 Region. Content is made available through an Amazon CloudFront origin pointing to that bucket. Cross-Region replication is set to create a second copy of the bucket in the ap-southeast-1 Region.
Management wants a solution that provides greater availability for the website.
Which combination of actions should a solutions architect take to increase availability? (Choose two.)

A. Add both buckets to the CloudFront origin.
B. Configure failover routing in Amazon Route 53.
C. Create a record in Amazon Route 53 pointing to the replica bucket.
D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket.
E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

Commented [LC210]: D,E are the answers
Ref:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html

Question #268

A company hosts a training site on a fleet of Amazon EC2 instances. The company anticipates that its new course, which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week.
What should a solutions architect do to minimize the anticipated server load?

A. Store the videos in Amazon ElastiCache for Redis. Update the web servers to serve the videos using the ElastiCache API.
B. Store the videos in Amazon Elastic File System (Amazon EFS). Create a user data script for the web servers to mount the EFS volume.
C. Store the videos in an Amazon S3 bucket. Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket. Restrict Amazon S3 access to the OAI.
D. Store the videos in an Amazon S3 bucket. Create an AWS Storage Gateway file gateway to access the S3 bucket. Create a user data script for the web servers to mount the file gateway.

Commented [LC211]: ANSWER

Question #269

A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.
Which solution meets these requirements MOST cost-effectively?

A. Use Spot Instances exclusively to handle the maximum capacity required.
B. Use Reserved Instances exclusively to handle the maximum capacity required.
C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Commented [LC212]: Without any downtime, the best combination is Reserved for the baseline and On-demand for the additional

Question #270

A company has a hybrid application hosted on multiple on-premises servers with static IP addresses. There is already a VPN that provides connectivity between the VPC and the on-premises network. The company wants to distribute TCP traffic across the on-premises servers for internet users.
What should a solutions architect recommend to provide a highly available and scalable solution?

A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB.
B. Launch an internet-facing Application Load Balancer (ALB) and register on-premises IP addresses with the ALB.
C. Launch an Amazon EC2 instance, attach an Elastic IP address, and distribute traffic to the on-premises servers.

Commented [LC213]: NLB is level-4, therefore the answer

D. Launch an Amazon EC2 instance with public IP addresses in an Auto Scaling group and distribute traffic to the on-premises servers.

Question #271

Management has decided to deploy all AWS VPCs with IPv6 enabled. After some time, a solutions architect tries to launch a new instance and receives an error stating that there is not enough IP address space available in the subnet.
What should the solutions architect do to fix this?

A. Check to make sure that only IPv6 was used during the VPC creation.
B. Create a new IPv4 subnet with a larger range, and then launch the instance.
C. Create a new IPv6-only subnet with a large range, and then launch the instance.
D. Disable the IPv4 subnet and migrate all instances to IPv6 only. Once that is complete, launch the instance.

Commented [LC214]: There are no IPV6-only subnets in AWS, therefore you must create a larger IPV4 subnet

Question #272

A company has a build server that is in an Auto Scaling group and often has multiple Linux instances running. The build server requires consistent and mountable shared NFS storage for jobs and configurations.
Which storage option should a solutions architect recommend?

A. Amazon S3
B. Amazon FSx
C. Amazon Elastic Block Store (Amazon EBS)
D. Amazon Elastic File System (Amazon EFS)

Commented [LC215]: A,C obviously wrong, B may be true but we look for NFS, not SMB.

D.

Question #273

A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets. Each private subnet uses a NAT instance for internet access. All images are stored in Amazon S3 buckets. The company is concerned about the data transfer costs between Amazon ECS and Amazon S3.
What should a solutions architect do to reduce costs?

A. Configure a NAT gateway to replace the NAT instances.
B. Configure a gateway endpoint for traffic destined to Amazon S3.
C. Configure an interface endpoint for traffic destined to Amazon S3.
D. Configure Amazon CloudFront for the S3 bucket storing the images.

Commented [LC216]: ANSWER

Question #274

The financial application at a company stores monthly reports in an Amazon S3 bucket. The vice president of finance has mandated that all access to these reports be logged and that any modifications to the log files be detected.
Which actions can a solutions architect take to meet these requirements?

A. Use S3 server access logging on the bucket that houses the reports with the read and write data events and log file validation options enabled.
B. Use S3 server access logging on the bucket that houses the reports with the read and write management events and log file validation options enabled.
C. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write data events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.
D. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.

Commented [LC217]: ANSWER

Question #275

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.
Which solution meets these requirements?

A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Commented [LC218]: To maintain local access to all the data means Stored Volume gateway

Question #276

A company is using a third-party vendor to manage its marketplace analytics. The vendor needs limited programmatic access to resources in the company's account. All the needed policies have been created to grant appropriate access.
Which additional component will provide the vendor with the MOST secure access to the account?

A. Create an IAM user.
B. Implement a service control policy (SCP)
C. Use a cross-account role with an external ID.
D. Configure a single sign-on (SSO) identity provider.

Commented [LC219]: D is for internal accounts only

Question #277

A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.
Which solutions meet these requirements? (Choose two.)

A. Create an Amazon RDS DB instance in Multi-AZ mode.
B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Commented [LC220]: ANSWER

Commented [LC221]: ANSWER

Question #278

A company has an ecommerce application that stores data in an on-premises SQL database. The company has decided to migrate this database to AWS. However, as part of the migration, the company wants to find a way to attain sub-millisecond responses to common read requests.
A solutions architect knows that the increase in speed is paramount and that a small percentage of stale data returned in the database reads is acceptable.
What should the solutions architect recommend?

A. Build Amazon RDS read replicas.
B. Build the database as a larger instance type.
C. Build a database cache using Amazon ElastiCache.
D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

Commented [LC222]: ANSWER

Question #279

A company has an application that ingests incoming messages. These messages are then quickly consumed by dozens of other applications and microservices. The number of messages varies drastically and sometimes spikes as high as 100,000 each second. The company wants to decouple the solution and increase scalability.
Which solution meets these requirements?

A. Persist the messages to Amazon Kinesis Data Analytics. All the applications will read and process the messages.
B. Deploy the application on Amazon EC2 instances in an Auto Scaling group, which scales the number of EC2 instances based on CPU metrics.
C. Write the messages to Amazon Kinesis Data Streams with a single shard. All applications will read from the stream and process the messages.
D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with one or more Amazon Simple Queue Service (Amazon SQS) subscriptions. All applications then process the messages from the queues.

Commented [LC223]: ANSWER

Question #280

A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users. During startup, the models need to load up to 10 GB of data from Amazon S3 into memory, but they do not need disk access. Most of the models are used sporadically, but the users expect all of them to be highly available and accessible with low latency.
Which solution meets the requirements and is MOST cost-effective?

A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model.
B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model.
C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.
D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model.

Commented [LC224]: D for high availability and path-based routing
Ref.
https://aws.amazon.com/it/premiumsupport/knowledge-center/elb-achieve-path-based-routing-alb/

Question #291

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.
Which additional configuration strategy should the solutions architect use to meet these requirements?

A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Commented [LC225]: ANSWER

Question #292

A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by a way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.
Which solution meets these requirements?

A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.
D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

Commented [LC226]: ALIAS is the AWS' solution for CNAME, so A is to be excluded, C and D don't make sense since we need a CNAME-LIKE record here. B is the answer

Question #293

A company owns an asynchronous API that is used to ingest user requests and, based on the request type, dispatch requests to the appropriate microservice for processing. The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices.
The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests.
What should a solutions architect do to address this issue without impacting existing users?

A. Add throttling on the API Gateway with server-side throttling limits.
B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
C. Create a secondary index in DynamoDB for the table with the user requests.
D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Commented [LC227]: ANSWER

Question #294

A company is moving its on-premises applications to Amazon EC2 instances. However, as a result of fluctuating compute requirements, the EC2 instances must always be ready to use between 8 AM and 5 PM in specific Availability Zones.
Which EC2 instances should the company choose to run the applications?

A. Scheduled Reserved Instances
B. On-Demand Instances
C. Spot Instances as part of a Spot Fleet
D. EC2 instances in an Auto Scaling group

Commented [LC228]: Before A would be correct. Now A is not possible anymore so you can use on-demand instances for the purpose. Hence, now it would be B. Probably this question was before the change that AWS made

Question #295

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.
What should a solutions architect recommend?

A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

Commented [LC229]: ANSWER

Question #296

A company is building an application on Amazon EC2 instances that generates temporary transactional data. The application requires access to data storage that can provide configurable and consistent IOPS.
What should a solutions architect recommend?

A. Provision an EC2 instance with a Throughput Optimized HDD (st1) root volume and a Cold HDD (sc1) data volume.
B. Provision an EC2 instance with a Throughput Optimized HDD (st1) volume that will serve as the root and data volume.
C. Provision an EC2 instance with a General Purpose SSD (gp2) root volume and Provisioned IOPS SSD (io1) data volume.
D. Provision an EC2 instance with a General Purpose SSD (gp2) root volume. Configure the application to store its data in an Amazon S3 bucket.

Commented [LC230]: ANSWER

Question #297

A solutions architect needs to design a resilient solution for Windows users' home directories. The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company's Active Directory.
Which storage solution meets these requirements?

A. Configure Amazon S3 to store the users' home directories. Join Amazon S3 to Active Directory.
B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server. Join Amazon FSx to Active Directory.
C. Configure Amazon Elastic File System (Amazon EFS) for the users' home directories. Configure AWS Single Sign-On with Active Directory.
D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users' home directories. Configure AWS Single Sign-On with Active Directory.

Commented [LC231]: ANSWER

Question #298

A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.
Which solution meets these requirements and is the MOST operationally efficient?

A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Commented [LC232]: ANSWER

Question #299

A company serves a multilingual website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). This architecture is currently running in the us-west-1 Region but is exhibiting high request latency for users located in other parts of the world.
The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.
How should a solutions architect accomplish this?

A. Replace the existing architecture with a website served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to only cache based on the Accept-Language request header.
C. Set up Amazon API Gateway with the ALB as an integration. Configure API Gateway to use an HTTP integration type. Set up an API Gateway stage to enable the API cache.
D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the instances plus the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Commented [LC233]: ANSWER

Question #300

A software vendor is deploying a new software-as-a-service (SaaS) solution that will be utilized by many AWS users. The service is hosted in a VPC behind a Network Load Balancer. The software vendor wants to provide access to this service to users with the least amount of administrative overhead and without exposing the service to the public internet.
What should a solutions architect do to accomplish this goal?

A. Create a peering VPC connection from each user's VPC to the software vendor's VPC.
B. Deploy a transit VPC in the software vendor's AWS account. Create a VPN connection with each user account.
C. Connect the service in the VPC with an AWS Private Link endpoint. Have users subscribe to the endpoint.
D. Deploy a transit VPC in the software vendor's AWS account. Create an AWS Direct Connect connection with each user account.

Commented [LC234]: ANSWER

Questions from 301-400

Question #301

A user wants to list the IAM role that is attached to their Amazon EC2 instance. The user has login access to the EC2 instance but does not have IAM permissions.
What should a solutions architect do to retrieve this information?

A. Run the following EC2 command: curl http://169.254.169.254/latest/meta-data/iam/info
B. Run the following EC2 command: curl http://169.254.169.254/latest/user-data/iam/info
C. Run the following EC2 command: http://169.254.169.254/latest/dynamic/instance-identity/
D. Run the following AWS CLI command: aws iam get-instance-profile --instance-profile-name ExampleInstanceProfile

Commented [LC235]: ANSWER

Question #302

A company has an application that is hosted on Amazon EC2 instances in two private subnets. A solutions architect must make the application available on the public internet with the least amount of administrative effort.
What should the solutions architect recommend?

A. Create a load balancer and associate two public subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
B. Create a load balancer and associate two private subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
C. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two public subnets from the same Availability Zones as the public instances.
D. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two private subnets from the same Availability Zones as the public instances.

Commented [LC236]: ANSWER

Question #303

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.
Which solution meets these requirements and is the MOST operationally efficient?

A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Commented [LC237]: ANSWER

Question #304

A company's website hosted on Amazon EC2 instances processes classified data stored in Amazon S3. Due to security concerns, the company requires a private and secure connection between its EC2 resources and Amazon S3.
Which solution meets these requirements?

A. Set up S3 bucket policies to allow access from a VPC endpoint.
B. Set up an IAM policy to grant read-write access to the S3 bucket.
C. Set up a NAT gateway to access resources outside the private subnet.
D. Set up an access key ID and a secret access key to access the S3 bucket.

Commented [LC238]: ANSWER

Question #305

A company hosts its multi-tier, public web application in the AWS Cloud. The web application runs on Amazon EC2 instances and its database runs on Amazon
RDS. The company is anticipating a large increase in sales during an upcoming holiday weekend. A solutions architect needs to build a solution to analyse the performance of the web application with a granularity of no more than 2 minutes.
What should the solutions architect do to meet this requirement?

A. Send Amazon CloudWatch logs to Amazon Redshift. Use Amazon QuickSight to perform further analysis.
B. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.
C. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform further analysis.
D. Send EC2 logs to Amazon S3. Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.

Commented [LC239]: ANSWER

Question #306

A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL. In the database layer several players will compete concurrently online. The game's developers want to display a top-10 scoreboard in near-real time and offer the ability to stop and restore the game while preserving the current scores.
What should a solutions architect do to meet these requirements?

A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.
B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.
C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.
D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

Commented [LC240]: https://aws.amazon.com/it/blogs/database/building-a-real-time-gaming-leaderboard-with-amazon-elasticache-for-redis/

Question #307

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.
What should a solutions architect recommend?

A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all cables.
B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
C. Use the AWS Schema Conversion Tool with AWS DataBase Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Commented [LC241]: ANSWER

Question #308

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity.
Which architecture offers the HIGHEST availability?

A. Add a second ActiveMQ server to another Availability Zone. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
B. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.
D. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

Commented [LC242]: ANSWER

Question #309

A company is planning on deploying a newly built application on AWS in a default VPC. The application will consist of a web layer and database layer. The web server was created in public subnets, and the MySQL database was created in private subnets. All subnets are created with the default network ACL settings, and the default security group in the VPC will be replaced with new custom security groups.
The following are the key requirements:
⇨ The web servers must be accessible only to users on an SSL connection.
⇨ The database should be accessible to the web layer, which is created in a public subnet only.
⇨ All traffic to and from the IP range 182.20.0.0/16 subnet should be blocked.
Which combination of steps meets these requirements? (Select two.)

A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0 0.0.0/0).
B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.

Commented [LC243]: ANSWER

C. Create a web server security group with an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182.20.0.0/16.
D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0). Create network ACL inbound and outbound deny rules for IP range 182.20.0.0/16.

Commented [LC244]: ANSWER

E. Create a web server security group with inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0). Create a network ACL inbound deny rule for IP range 182.20.0.0/16.

Question #310

A company has an on-premises application that collects data and stores it to an on-premises NFS server. The company recently set up a 10 Gbps AWS Direct Connect connection. The company is running out of storage capacity on premises. The company needs to migrate the application data from on premises to the AWS Cloud while maintaining low-latency access to the data from the on-premises application.
What should a solutions architect do to meet these requirements?

A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3. Connect the on-premises application servers to the file gateway using NFS.

Commented [LC245]: You can use a combination of DataSync and File Gateway to minimize your on-premises' operational costs while seamlessly connecting on-premises applications to your cloud storage. AWS DataSync enables you to automate and accelerate online data transfers to AWS storage services. File Gateway then provides your on-premises applications with low latency access to the migrated data.

In this case, low latency is the key

B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server, and copy the application data to the EFS file system. Then connect the on-premises application to Amazon EFS.
C. Configure AWS Storage Gateway as a volume gateway. Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots.
D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer. Connect the on-premises application to the EFS file system.

Question #311

A solutions architect needs to design a network that will allow multiple Amazon EC2 instances to access a common data source used for mission-critical data that can be accessed by all the EC2 instances simultaneously. The solution must be highly scalable, easy to implement and support the NFS protocol.
Which solution meets these requirements?

A. Create an Amazon Elastic File System (Amazon EFS) file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.
B. Create an additional EC2 instance and configure it as a file server. Create a security group that allows communication between the Instances and apply that to the additional instance.
C. Create an Amazon S3 bucket with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the S3 bucket. Attach the role to the EC2 Instances that need access to the data.
D. Create an Amazon Elastic Block Store (Amazon EBS) volume with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the EBS volume. Attach the role to the EC2 instances that need access to the data.

Commented [LC246]: ANSWER

Question #312

A company hosts its application using Amazon Elastic Container Service (Amazon ECS) and wants to ensure high availability. The company wants to be able to deploy updates to its application even if nodes in one Availability Zone are not accessible.
The expected request volume for the application is 100 requests per second, and each container task is able to serve at least 60 requests per second. The company set up Amazon ECS with a rolling update deployment type with the minimum healthy percent parameter set to 50% and the maximum percent set to 100%.
Which configuration of tasks and Availability Zones meets these requirements?

A. Deploy the application across two Availability Zones, with one task in each Availability Zone.
B. Deploy the application across two Availability Zones, with two tasks in each Availability Zone.
C. Deploy the application across three Availability Zones, with one task in each Availability Zone.
D. Deploy the application across three Availability Zones, with two tasks in each Availability Zone.

Commented [LC247]: We need at least 50% of nodes for updating
We need to guarantee this 50% even if one AZ is down
We need to guarantee at least 100 req / s

With 3 AZ and 2 Tasks each:
If one AZ is down, meaning 2/6 tasks is down, we still have 4/6 tasks available. For updating, we need 50% of tasks, so 2/6. We have 2/6 tasks for the rest. 2 Tasks can do 60*2 req/s which is > than 100 req/s so all objectives are reached.

Answer is D.

Question #313

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords. What should the solutions architect do to accomplish this?

A. Set an overall password policy for the entire AWS account
B. Set a password policy for each IAM user in the AWS account.
C. Use third-party vendor software to set password requirements.
D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Commented [LC248]: ANSWER

Question #314

A company wants to improve the availability and performance of its hybrid application. The application consists of a stateful TCP-based workload hosted on Amazon EC2 instances in different AWS Regions and a stateless UDP-based workload hosted on premises.
Which combination of actions should a solutions architect take to improve availability and performance? (Choose two.)

A. Create an accelerator using AWS Global Accelerator. Add the load balancers as endpoints.
B. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the load balancers.
C. Configure two Application Load Balancers in each Region. The first will route to the EC2 endpoints and the second will route to the on-premises endpoints.
D. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure a Network Load Balancer in each Region that routes to the on- premises endpoints.
E. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure an Application Load Balancer in each Region that routes to the on-premises endpoints.

Commented [LC249]: This is good for accelerating UDP (so performance) traffic.

Commented [LC250]: NLB is level-4, useful for taking care also of on-prem endpoints

Question #315

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.
What should the solutions architect do to ensure that the architecture supports distributed session data management?

A. Use Amazon ElastiCache to manage and store session data.
B. Use session affinity (sticky sessions) of the ALB to manage session data.
C. Use Session Manager from AWS Systems Manager to manage the session.
D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session.

Commented [LC251]: ANSWER

Question #316

A company has an ecommerce application running in a single VPC. The application stack has a single web server and an Amazon RDS Multi-AZ DB instance.

The company launches new products twice a month. This increases website traffic by approximately 400% for a minimum of 72 hours. During product launches, users experience slow response times and frequent timeout errors in their browsers.

What should a solutions architect do to mitigate the slow response times and timeout errors while minimizing operational overhead?

A. Increase the instance size of the web server.
B. Add an Application Load Balancer and an additional web server.
C. Add Amazon EC2 Auto Scaling and an Application Load Balancer.
D. Deploy an Amazon ElastiCache cluster to store frequently accessed data.

Commented [LC252]: A is a temporary solution, bad also because it's not horizontal scaling. B is a temporary solution. D doesn't make sense since there's no frequent data to be accessed. C makes sense.

Question #317

A solutions architect is designing an architecture to run a third-party database server. The database software is memory intensive and has a CPU-based licensing model where the cost increases with the number of vCPU cores within the operating system. The solutions architect must select an Amazon EC2 instance with sufficient memory to run the database software, but the selected instance has a large number of vCPUs. The solutions architect must ensure that the vCPUs will not be underutilized and must minimize costs.

Which solution meets these requirements?

A. Select and launch a smaller EC2 instance with an appropriate number of vCPUs.
B. Configure the CPU cores and threads on the selected EC2 instance during instance launch.
C. Create a new EC2 instance and ensure multithreading is enabled when configuring the instance details.
D. Create a new Capacity Reservation and select the appropriate instance type. Launch the instance into this new Capacity Reservation.

Commented [LC253]: ANSWER

Question #318

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive.

Which solution offers the MOST reliable data transfer?

A. AWS DataSync over public internet
B. AWS DataSync over AWS Direct Connect
C. AWS Database Migration Service (AWS DMS) over public internet
D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Commented [LC254]: It's not a migration so C,D are out. A is not secure since it's over public internet.

Question #319

A company is creating a web application that will store a large number of images in Amazon S3. The images will be accessed by users over variable periods of time. The company wants to:

➾ Retain all the images
➾ Incur no cost for retrieval.
➾ Have minimal management overhead.
➾ Have the images available with no impact on retrieval time.

Which solution meets these requirements?

A. Implement S3 Intelligent-Tiering
B. Implement S3 storage class analysis
C. Implement an S3 Lifecycle policy to move data to S3 Standard-Infrequent Access (S3 Standard-IA).
D. Implement an S3 Lifecycle policy to move data to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Commented [LC255]: ANSWER

Question #320

A company hosts more than 300 global websites and applications. The company requires a platform to analyse more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Commented [LC256]: ANSWER

Question #321

A company wants to build an online marketplace application on AWS as a set of loosely coupled microservices. For this application, when a customer submits a new order, two microservices should handle the event simultaneously. The Email microservice will send a confirmation email, and the OrderProcessing microservice will start the order delivery process. If a customer cancels an order, the OrderCancelation and Email microservices should handle the event simultaneously.
A solutions architect wants to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) to design the messaging between the microservices.
How should the solutions architect design the solution?

A. Create a single SQS queue and publish order events to it. The Email OrderProcessing and Order Cancellation microservices can then consume messages of the queue.
B. Create three SNS topics for each microservice. Publish order events to the three topics. Subscribe each of the Email OrderProcessing and Order Cancellation microservices to its own topic.
C. Create an SNS topic and publish order events to it. Create three SQS queues for the Email OrderProcessing and Order Cancellation microservices. Subscribe all SQS queues to the SNS topic with message filtering.
D. Create two SQS queues and publish order events to both queues simultaneously. One queue is for the Email and OrderProcessing microservices. The second queue is for the Email and Order Cancellation microservices.

Commented [LC257]: ANSWER

Question #322

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 Instances with an Amazon RDS MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation instance with 2,000 GB of storage in an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume. The database performance impacts the application during periods of high demand.
After analysing the logs in Amazon CloudWatch Logs, a database administrator finds that the application performance always degrades when the number of read and write IOPS is higher than 6.000.
What should a solutions architect do to improve the application performance?

A. Replace the volume with a Magnetic volume.
B. Increase the number of IOPS on the gp2 volume.
C. Replace the volume with a Provisioned IOPS (PIOPS) volume.
D. Replace the 2,000 GB gp2 volume with two 1,000 GBgp2 volumes.

Commented [LC258]: ANSWER

Question #323

A company has an application that uses Amazon Elastic File System (Amazon EFS) to store data. The files are 1 GB in size or larger and are accessed often only for the first few days after creation. The application data is shared across a cluster of Linux servers. The company wants to reduce storage costs tor the application.
What should a solutions architect do to meet these requirements?

A. Implement Amazon FSx and mount the network drive on each server.
B. Move the files from Amazon Elastic File System (Amazon EFS) and store them locally on each Amazon EC2 instance.
C. Configure a Lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7 days.
D. Move the files to Amazon S3 with S3 lifecycle policies enabled. Rewrite the application to support mounting the S3 bucket.

Commented [LC259]: ANSWER

Question #324

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.
How should a solution architect accomplish this?

A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Commented [LC260]: ANSWER

Question #325

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.
What should the company do to guarantee the EC2 capacity?

A. Purchase Reserved Instances that specify the Region needed.
B. Create an On-Demand Capacity Reservation that specifies the Region needed.
C. Purchase Reserved Instances that specify the Region and three Availability Zones needed.
D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

Commented [LC261]: ANSWER

Question #326

A company wants to migrate its web application to AWS. The legacy web application consists of a web tier, an application tier, and a MySQL database. The re-architected application must consist of technologies that do not require the administration team to manage instances or clusters.
Which combination of services should a solutions architect include in the overall architecture? (Choose two.)

A. Amazon Aurora Serverless
B. Amazon EC2 Spot Instances
C. Amazon Elasticsearch Service (Amazon ES)
D. Amazon RDS for MySQL
E. AWS Fargate

Commented [LC262]: ANSWER

Commented [LC263]: ANSWER

Question #327

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier two application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.
What should a solutions architect do to meet these requirements?

A. Create a separate application tier using EC2 instances dedicated to email processing.
B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).
D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Commented [LC264]: ANSWER

Question #328

A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPU Utilization metrics are spiking when monthly reports run.
What is the MOST cost-effective solution?

A. Migrate the monthly reporting to Amazon Redshift.
B. Migrate the monthly reporting to an Aurora Replica.
C. Migrate the Aurora database to a larger instance class.
D. Increase the Provisioned IOPS on the Aurora instance.

Commented [LC265]: ANSWER

Question #329

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.
Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

A. Mount Amazon S3 as a file system to the on-premises servers.
B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
E. Deploy Amazon Elastic Fife System (Amazon EFS) volumes and mount them to on-premises servers.

Commented [LC266]: ANSWER

Commented [LC267]: ANSWER

Question #330

A solution architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.
Which solution meets these requirements and is MOST secure?

A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
B. Amazon EC2 instances in private subnets Configure. Configure a public Application Load Balancer with multiple redundant Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Commented [LC268]: ANSWER

Question #331

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.
Which solution meets these requirements?

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in- memory cache for DynamoDB hosting the application data.

Commented [LC269]: ANSWER

Question #332

A company is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in Amazon RDS MySQL Multi-AZ DB instances. The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks.
What should a solutions architect recommend?

A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Configure the EC2 instance iptables rules to drop suspicious web traffic. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Move DB instances to the same subnets that EC2 instances are located in. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.
D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Configure the Auto Scaling group to automatically create new DB instances under heavy traffic. Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

Commented [LC270]: ANSWER

Question #333

A development team stores its Amazon RDS MySQL DB instance user name and password credentials in a configuration file. The configuration file is stored as plaintext on the root device volume of the team's Amazon EC2 instance. When the team's application needs to reach the database, it reads the file and loads the credentials into the code. The team has modified the permissions of the configuration file so that only the application can read its content. A solution architect must design a more secure solution.
What should the solutions architect do to meet this requirement?

A. Store the configuration file in Amazon S3. Grant the application access to read the configuration file.
B. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.
C. Enable SSL connections on the database instance. Alter the database user to require SSL when logging in.
D. Move the configuration file to an EC2 instance store, and create an Amazon Machine Image (AMI) of the instance. Launch new instances from this AMI.

Commented [LC271]: ANSWER

Question #334

A company wants a storage option that enables its data science team to analyse its data on premises and in the AWS Cloud. The team needs to be able to run statistical analyses by using the data on premises and by using a fleet of Amazon EC2 instances across multiple Availability Zones.
What should a solutions architect do to meet these requirements?

A. Use an AWS Storage Gateway tape gateway to copy the on-premises files into Amazon S3.
B. Use an AWS Storage Gateway volume gateway to copy the on-premises files into Amazon S3.
C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store (Amazon EBS).
D. Attach an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers. Copy the files to Amazon EFS.

Commented [LC272]: ANSWER

Question #335

A company wants to improve the availability and performance of its stateless UDP-based workload. The workload is deployed on Amazon EC2 instances in multiple AWS Regions.
What should a solutions architect recommend to accomplish this?

A. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the NLBs as endpoints for the accelerator.
B. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the ALBs as endpoints for the accelerator.
C. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the NLBs.
D. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs.

Commented [LC273]: ANSWER

Question #336

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.
The company seeks a cloud storage solution that permits the copying of on premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.
Which combination of AWS services meets these requirements?

A. Amazon FSx for Lustre integrated with Amazon S3
B. Amazon FSx for Windows File Server integrated with Amazon S3
C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Commented [LC274]: FSx for Lustre is used for HCP purposes

Question #337

A solutions architect must design a database solution for a high-traffic ecommerce web application. The database stores customer profiles and shopping cart information. The database must support a peak load of several million requests each second and deliver responses in milliseconds. The operational overhead form an aging and scaling the database must be minimized.
Which database solution should the solutions architect recommend?

A. Amazon Aurora
B. Amazon DynamoDB
C. Amazon RDS
D. Amazon Redshift

Commented [LC275]: Why not Aurora?

Question #338

A company is working with an external vendor that requires write access to the company's Amazon Simple Queue Service (Amazon SQS) queue. The vendor has its own AWS account.
What should a solutions architect do to implement least privilege access?

A. Update the permission policy on the SQS queue to give write access to the vendor's AWS account.
B. Create an IAM user with write access to the SQS queue and share the credentials for the IAM user.
C. Update AWS Resource Access Manager to provide write access to the SQS queue from the vendor's AWS account.
D. Create a cross-account role with access to all SQS queues and use the vendor's AWS account in the trust document for the role.

Commented [LC276]: You can do it via the console under "Define who can send messages to the queue"

Question #339

A company is creating a three-tier web application consisting of a web server, an application server, and a database server. The application will track GPS coordinates of packages as they are being delivered. The application will update the database every 0-5 seconds.
The tracking will need to read a fast as possible for users to check the status of their packages. Only a few packages might be tracked on some days, whereas millions of package might be tracked on other days. Tracking will need to be searchable by tracking ID customer ID and order ID.
Order than 1 month no longer read to be tracked.
What should a solution architect recommend to accomplish this with minimal cost of ownership?

A. Use Amazon DynamoDB Enable Auto Scaling on the DynamoDB table. Schedule an automatic deletion script for items older than 1 month.
B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.
C. Use an Amazon RDS On-Demand instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.
D. Use an Amazon RDS Reserved Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notification when PIOPS are exceeded. Increase and decrease PIOPS as needed.

Commented [LC277]: ANSWER

Question #340

A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete. If the job is interrupted, it has to restart from the beginning.
How should the solutions architect address this issue in the MOST cost-effective manner?

A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.
B. Create an AWS Lambda function triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.

Commented [LC278]: ANSWER

Question #341

A company needs to store data in Amazon S3. A compliance requirement states that when any changes are made to objects the previous state of the object with any changes must be preserved. Additionally, files older than 5 years should not be accessed but need to be archived for auditing.
What should a solutions architect recommend that is MOST cost-effective?

A. Enable object-level versioning and S3 Object Lock in governance mode
B. Enable object-level versioning and S3 Object Lock in compliance mode
C. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Glacier Deep Archive
D. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Standard-Infrequent Access (S3 Standard-IA)

Commented [LC279]: ANSWER

Question #342

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.
Which combination of actions should the solutions architect take to accomplish this goal? (Choose two.)

A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.
D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

Commented [LC280]: ANSWER

Question #343

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings in the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur they will happen very quickly.
What should a solutions architect recommend?

A. Create a DynamoDB table in on-demand capacity mode.
B. Create a DynamoDB table with a global secondary Index.
C. Create a DynamoDB table with provisioned capacity and auto scaling.
D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Commented [LC281]: ANSWER

Question #344

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.
What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?

A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Commented [LC282]: ANSWER

Question #345

A company is preparing to deploy a new serverless workload. A solutions architect needs to configure permissions for invoking an AWS Lambda function. The function will be triggered by an Amazon EventBridge (Amazon CloudWatch Events) rule. Permissions should be configured using the principle of least privilege.
Which solution will meet these requirements?

A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
B. Add an execution role to the function with lambda:InvokeFunction as the action and Service:amazonaws.com as the principal.
C. Add a resource-based policy to the function with lambda:* as the action and Service:events.amazonaws.com as the principal.
D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.

Commented [LC283]: ANSWER

Question #346

A company is building its web application using containers on AWS. The company requires three instances of the web application to run at all times. The application must be able to scale to meet increases in demand. Management is extremely sensitive to cost but agrees that the application should be highly available.
What should a solutions architect recommend?

A. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
B. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
C. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type with one container instance in three different Availability Zones. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance and one task on the remaining container instance.

Commented [LC284]: ANSWER

Question #347

A company is Re-architecting a strongly coupled application to be loosely coupled. Previously the application used a request/response pattern to communicate between tiers. The company plans to use Amazon Simple Queue Service (Amazon SQS) to achieve decoupling requirements. The initial design contains one queue for requests and one for responses. However, this approach is not processing all the messages as the application scales.
What should a solutions architect do to resolve this issue?

A. Configure a dead-letter queue on the ReceiveMessage API action of the SQS queue.
B. Configure a FIFO queue, and use the message deduplication ID and message group ID.
C. Create a temporary queue, with the Temporary Queue Client to receive each response message.
D. Create a queue for each request and response on startup for each producer, and use a correlation ID message attribute.

Commented [LC285]: ANSWER

Question #348

A company is launching an ecommerce website on AWS. This website is built with a three-tier architecture that includes a MySQL database in a Multi-AZ deployment of Amazon Aurora MySQL. The website application must be highly available and will initially be launched in an AWS Region with three Availability Zones The application produces a metric that describes the load the application experiences.
Which solution meets these requirements?

A. Configure an Application Load Balancer (ALB) with Amazon EC2 Auto Scaling behind the ALB with scheduled scaling
B. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a simple scaling policy.
C. Configure a Network Load Balancer (NLB) and launch a Spot Fleet with Amazon EC2 Auto Scaling behind the NLB.
D. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a target tracking scaling policy.

Commented [LC286]: ANSWER

Question #349

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.
Which action should the solutions architect take?

A. Configure a CloudFront signed URL
B. Configure a CloudFront signed cookie.
C. Configure a CloudFront field-level encryption profile.
D. Configure a CloudFront and set the Origin Protocol Policy setting to HTTPS. Only for the Viewer Protocol Pokey.

Commented [LC287]: ANSWER

Question #350

A solutions architect is redesigning a monolithic application to be a loosely coupled application composed of two microservices: Microservice A and Microservice B.

Microservice A places messages in a main Amazon Simple Queue Service (Amazon SQS) queue for Microservice B to consume. When Microservice B fails to process a message after four retries, the message needs to be removed from the queue and stored for further investigation.

What should the solutions architect do to meet these requirements?

A. Create an SQS dead-letter queue. Microservice B adds failed messages to that queue after it receives and fails to process the message four times.
B. Create an SQS dead-letter queue. Configure the main SQS queue to deliver messages to the dead-letter queue after the message has been received four times.
C. Create an SQS queue for failed messages. Microservice A adds failed messages to that queue after Microservice B receives and fails to process the message four times.
D. Create an SQS queue for failed messages. Configure the SQS queue for failed messages to pull messages from the main SQS queue after the original message has been received four times.

Commented [LC288]: It's the queue that moves the messages to the DLQ

Question #351

A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3. Which solution meets these requirements and is MOST cost-effective?

A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.
B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.
C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on-premises to Amazon S3.
D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

Commented [LC289]: ANSWER

Question #352

A company runs its production workload on an Amazon Aurora MySQL DB cluster that includes six Aurora Replicas. The company wants near-real-time reporting queries from one of its departments to be automatically distributed across three of the Aurora Replicas. Those three replicas have a different compute and memory specification from the rest of the DB cluster.

Which solution meets these requirements?

A. Create and use a custom endpoint for the workload.
B. Create a three-node cluster clone and use the reader endpoint.
C. Use any of the instance endpoints for the selected three nodes.
D. Use the reader endpoint to automatically distribute the read-only workload.

Commented [LC290]: ANSWER

Question #353

A company has multiple applications that use Amazon RDS for MySQL as is database. The company recently discovered that a new custom reporting application has increased the number of Queries on the database. This is slowing down performance.

How should a solutions architect resolve this issue with the LEAST amount of application changes?

A. Add a secondary DB instance using Multi-AZ.
B. Set up a read replica and Multi-AZ on Amazon RDS.
C. Set up a standby replica and Multi-AZ on Amazon RDS.
D. Use caching on Amazon RDS to improve the overall performance.

Commented [LC291]: ANSWER

Question #354

A company wants to automate the security assessment of its Amazon EC2 instances. The company needs to validate and demonstrate that security and compliance standards are being followed throughout the development process.

What should a solutions architect do to meet these requirements?

A. Use Amazon Macie to automatically discover, classify and protect the EC2 instances.
B. Use Amazon GuardDuty to publish Amazon Simple Notification Service (Amazon SNS) notifications.
C. Use Amazon Inspector with Amazon CloudWatch to publish Amazon Simple Notification Service (Amazon SNS) notifications
D. Use Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes in the status of AWS Trusted Advisor checks.

Commented [LC292]: ANSWER

Question #355

A company stores 200 GB of data each month in Amazon S3. The company needs to perform analytics on this data at the end of each month to determine the number of items sold in each sales region for the previous month.
Which analytics strategy is MOST cost-effective for the company to use?

A. Create an Amazon Elasticsearch Service (Amazon ES) cluster. Query the data in Amazon ES. Visualize the data by using Kibana.
B. Create a table in the AWS Glue Data Catalog. Query the data in Amazon S3 by using Amazon Athena. Visualize the data in Amazon QuickSight.
C. Create an Amazon EMR cluster. Query the data by using Amazon EMR, and store the results in Amazon S3. Visualize the data in Amazon QuickSight.
D. Create an Amazon Redshift cluster. Query the data in Amazon Redshift, and upload the results to Amazon S3. Visualize the data in Amazon QuickSight.

Commented [LC293]: I would go with C. A, B are wrong. D should be wrong too because it doubles the storage required for the files (store in RedShift, store in S3). C seems fine.

Question #356

A company wants to move its on-premises network, attached storage (NAS) to AWS. The company wants to make the data available to any Linux instances within its VPC and ensure changes are automatically synchronized across all instances accessing the data store. The majority of the data is accessed very rarely, and some files are accessed by multiple users at the same time.
Which solution meets these requirements and is MOST cost-effective?

A. Create an Amazon Elastic Block Store (Amazon EBS) snapshot containing the data. Share it with users within the VPC.
B. Create an Amazon S3 bucket that has a lifecycle policy set to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after the appropriate number of days.
C. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the throughput mode to Provisioned and to the required amount of IOPS to support concurrent usage.
D. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the lifecycle policy to transition the data to EFS Infrequent Access (EFS IA) after the appropriate number of days.

Commented [LC294]: ANSWER

Question #357

A company plans to host a survey website on AWS. The company anticipates an unpredictable amount of traffic. This traffic results in asynchronous updates to the database. The company wants to ensure that writes to the database hosted on AWS do not get dropped.
How should the company write its application to handle these database requests?

A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.
B. Configure the application to subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Publish the database updates to the SNS topic.
C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the database connection until the database has resources to write the data.
D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues for capturing the writes and draining the queue as each write is made to the database.

Commented [LC295]: ANSWER

Question #358

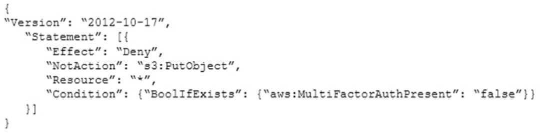
A company that recently started using AWS establishes a Site-to-Site VPN between its on-premises datacenter and AWS. The company's security mandate states that traffic originating from on premises should stay within the company's private IP space when communicating with an Amazon Elastic Container Service (Amazon ECS) cluster that is hosting a sample web application.
Which solution meets this requirement?

A. Configure a gateway endpoint for Amazon ECS. Modify the route table to include an entry pointing to the ECS cluster.
B. Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the same VPC that is hosting the ECS cluster.
C. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC. Connect the two VPCs by using VPC peering.
D. Configure an Amazon Route 53 record with Amazon ECS as the target. Apply a server certificate to Route 53 from AWS Certificate Manager (ACM) for SSL offloading.

Commented [LC296]: A, D wrong. C is B with extra steps. Therefore, the answer is B

Question #359

A solutions architect must analyse and update a company's existing IAM policies prior to deploying a new workload. The solutions architect created the following policy:



```
{
"Version": "2012-10-17",
   "Statement": [{
      "Effect": "Deny",
      "NotAction": "s3:PutObject",
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": "false"}}
   }]
}
```

What is the net effect of this policy?

A. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
B. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.
C. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
D. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.

Commented [LC297]: ANSWER

Question #360

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.
Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

A. Migrate the PostgreSQL database to Amazon Aurora.
B. Migrate the web application to be hosted on Amazon EC2 instances.
C. Set up an Amazon CloudFront distribution for the web application content.
D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Commented [LC298]: ANSWER

Commented [LC299]: ANSWER

Question #361

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.
What should the solutions architect recommend?

A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Commented [LC300]: ANSWER

Question #362

A company is using Amazon DynamoDB with provisioned throughput for the database tier of its ecommerce website. During flash sales, customers experience periods of time when the database cannot handle the high number of transactions taking place. This causes the company to lose transactions. During normal periods, the database performs appropriately.
Which solution solves the performance problem the company faces?

A. Switch DynamoDB to on-demand mode during flash sales.
B. Implement DynamoDB Accelerator for fast in memory performance.
C. Use Amazon Kinesis to queue transactions for processing to DynamoDB.
D. Use Amazon Simple Queue Service (Amazon SQS) to queue transactions to DynamoDB.

Commented [LC301]: ANSWER

Question #363

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.
What should a solutions architect do to correct this issue?

A. Create security group rules using the instance ID as the source or destination.
B. Create security group rules using the security group ID as the source or destination.
C. Create security group rules using the VPC CIDR blocks as the source or destination.
D. Create security group rules using the subnet CIDR blocks as the source or destination.

Commented [LC302]: ANSWER

Question #364

A company requires that all versions of objects in its Amazon S3 bucket be retained. Current object versions will be frequently accessed during the first 30 days, after which they will be rarely accessed and must be retrievable within 5 minutes. Previous object versions need to be kept forever, will be rarely accessed, and can be retrieved within 1 week. All storage solutions must be highly available and highly durable.
What should a solutions architect recommend to meet these requirements in the MOST cost-effective manner?

A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.
B. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
C. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Standard-infrequent Access (S3 Standard-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
D. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.

Commented [LC303]: Glacier: retrieval in minutes or hours
Deep Archive: retrieval in hours

Question #365

A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so.
How should a solutions architect provide access to the SQS queue?

A. Create an instance profile that provides the other company access to the SQS queue.
B. Create an IAM policy that provides the other company access to the SQS queue.
C. Create an SQS access policy that provides the other company access to the SQS queue.
D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

Commented [LC304]: ANSWER

Question #366

A company is developing a video conversion application hosted on AWS. The application will be available in two tiers: a free tier and a paid tier. Users in the paid tier will have their videos converted first and then the tree tier users will have their videos converted.
Which solution meets these requirements and is MOST cost-effective?

A. One FIFO queue for the paid tier and one standard queue for the free tier.
B. A single FIFO Amazon Simple Queue Service (Amazon SQS) queue for all file types.
C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all file types.
D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier.

Commented [LC305]: There's no need of FIFO. Answer is D. C is wrong as well because one Queue is not enough.

Question #367

An administrator of a large company wants to monitor for and prevent any cryptocurrency-related attacks on the company's AWS accounts.
Which AWS service can the administrator use to protect the company against attacks?

A. Amazon Cognito
B. Amazon GuardDuty
C. Amazon Inspector
D. Amazon Macie

Commented [LC306]: Macie is for Machine Learning. Cognito is for authentication. Inspector is for checking account's security from the requirements' side. GuardDuty is for actively protecting and monitoring the account.

Question #368

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However, the company's security policy states that any external service cannot initiate a connection to the EC2 instances. What should a solutions architect recommend to resolve this issue?

A. Create a NAT gateway and make it the destination of the subnet's route table.
B. Create an internet gateway and make it the destination of the subnet's route table.
C. Create a virtual private gateway and make it the destination of the subnet's route table.
D. Create an egress-only internet gateway and make it the destination of the subnet's route table.

Commented [LC307]: ANSWER

Question #369

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.
Which storage solution is MOST cost-effective?

A. Use AWS Storage Gateway for files to store and process the video content.
B. Use AWS Storage Gateway for volumes to store and process the video content.
C. Use Amazon Elastic File System (Amazon EFS) for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).

D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon ElasticBlock Store (Amazon EBS) volume attached to the server for processing.

Commented [LC308]: ANSWER

Question #370

A company wants to host its web application on AWS using multiple Amazon EC2 instances across different AWS Regions. Since the application content will be specific to each geographic region, the client requests need to be routed to the server that hosts the content for that clients Region.
What should a solutions architect do to accomplish this?

A. Configure Amazon Route 53 with a latency routing policy.
B. Configure Amazon Route 53 with a weighted routing policy.
C. Configure Amazon Route 53 with a geolocation routing policy.
D. Configure Amazon Route 53 with a multivalue answer routing policy

Commented [LC309]: ANSWER

Question #371

A solutions architect is planning the deployment of a new static website. The solution must minimize costs and provide at least 99% availability.
Which solution meets these requirements?

A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.
B. Deploy the application to Amazon EC2 instances that run in two AWS Regions and two Availability Zones.
C. Deploy the application to an Amazon S3 bucket that has versioning and cross-Region replication enabled.
D. Deploy the application to an Amazon EC2 instance that runs in one AWS Region and one Availability Zone.

Commented [LC310]: ANSWER

Question #372

A recently created startup built a three-tier web application. The front end has static content. The application layer is based on microservices. User data is stored as JSON documents that need to be accessed with low latency. The company expects regular traffic to be low during the first year, with peaks in traffic when it publicizes new features every month. The startup team needs to minimize operational overhead costs.
What should a solutions architect recommend to accomplish this?

A. Use Amazon S3 static website hosting to store and serve the front end. Use AWS Elastic Beanstalk for the application layer. Use Amazon DynamoDB to store user data.
B. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon Elastic KubernetesService (Amazon EKS) for the application layer. Use Amazon DynamoDB to store user data.
C. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon DynamoDB to store user data.
D. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon RDS with read replicas to store user data.

Commented [LC311]: ANSWER

Question #373

A company is building a payment application that must be highly available even during regional service disruptions. A solutions architect must design a data storage solution that can be easily replicated and used in other AWS Regions. The application also requires low-latency atomicity, consistency, isolation, and durability (ACID) transactions that need to be immediately available to generate reports. The development team also needs to use SQL.
Which data storage solution meets these requirements?

A. Amazon Aurora Global Database
B. Amazon DynamoDB global tables
C. Amazon S3 with cross-Region replication and Amazon Athena
D. MySQL on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) snapshot replication

Commented [LC312]: ANSWER

Question #374

A company stores call recordings on a monthly basis. Statistically, the recorded data may be referenced randomly within a year but accessed rarely after 1 year.
Files that are newer than 1 year old must be queried and retrieved as quickly as possible. A delay in retrieving older files is acceptable. A solutions architect needs to store the recorded data at a minimal cost.
Which solution is MOST cost-effective?

A. Store individual files in Amazon S3 Glacier and store search metadata in object tags created in S3 Glacier Query S3 Glacier tags and retrieve the files from S3 Glacier.
B. Store individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files from Amazon S3 or S3 Glacier.
C. Archive individual files and store search metadata for each archive in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
D. Archive individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Store search metadata in Amazon DynamoDB. Query the files from DynamoDB and retrieve them from Amazon S3 or S3 Glacier.

Commented [LC313]: ANSWER

Question #375

A company is developing a new machine learning model solution in AWS. The models are developed as independent microservices that fetch about 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which solution meets these requirements?

A. The requests from the API are sent to an Application Load Balancer (ALB). Models are deployed as AWS Lambda functions invoked by the ALB.

B. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as AWS Lambda functions triggered by SQS events AWS Auto Scaling is enabled on Lambda to increase the number of vCPUs based on the SQS queue size.

C. The requests from the API are sent to the model's Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS App Mesh scales the instances of the ECS cluster based on the SQS queue size.

D. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS Auto Scaling is enabled on Amazon ECS for both the cluster and copies of the service based on the queue size.

Commented [LC314]: ANSWER

Question #376

A company has no existing file share services. A new project requires access to file storage that is mountable as a drive for on-premises desktops. The file server must authenticate users to an Active Directory domain before they are able to access the storage.

Which service will allow Active Directory users to mount storage as a drive on their desktops?

A. Amazon S3 Glacier

B. AWS DataSync

C. AWS Snowball Edge

D. AWS Storage Gateway

Commented [LC315]: ANSWER

Question #377

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against largescale DDoS attacks.

Which solution meets these requirements?

A. Enable Amazon GuardDuty on the account.

B. Enable Amazon Inspector on the EC2 instances.

C. Enable AWS Shield and assign Amazon Route 53 to it.

D. Enable AWS Shield Advanced and assign the ELB to it.

Commented [LC316]: ANSWER

Question #378

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.

B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.

C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.

Commented [LC317]: ANSWER

D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Question #379

A company is running a multi-tier web application on AWS. The application runs its database tier on Amazon Aurora MySQL. The application and database tiers are in the us-east-1 Region. A database administrator who regularly monitors the Aurora DB cluster finds that an intermittent increase in read traffic is creating high CPU utilization on the read replica and causing increased read latency of the application.

What should a solutions architect do to improve read scalability?

A. Reboot the Aurora DB cluster.

B. Create a cross-Region read replica

C. Increase the instance class of the read replica.

D. Configure Aurora Auto Scaling for the read replica.

Commented [LC318]: ANSWER

Question #380

A company's order fulfilment service uses a MySQL database. The database needs to support a large number of concurrent queries and transactions. Developers are spending time patching and tuning the database This is causing delays in releasing new product features.
The company wants to use cloud-based services to help address this new challenge. The solution must allow the developers to migrate the database with little or no code changes and must optimize performance.
Which service should a solutions architect use to meet these requirements?

A. Amazon Aurora
B. Amazon DynamoDB
C. Amazon ElastiCache
D. MySQL on Amazon EC2

Commented [LC319]: ANSWER

Question #381

A company is planning to transfer multiple terabytes of data to AWS. The data is collected offline from ships. The company want to run complex transformation before transferring the data.
Which AWS service should a solutions architect recommend for this migration?

A. AWS Snowball
B. AWS Snowmobile
C. AWS Snowball Edge Storage Optimize
D. AWS Snowball Edge Compute Optimize

Commented [LC320]: ANSWER

Question #382

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.
What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

Commented [LC321]: ANSWER

Question #383

A company is selling up an application to use an Amazon RDS MySQL DB instance. The database must be architected for high availability across Availability Zones and AWS Regions with minimal downtime.
How should a solutions architect meet this requirement?

A. Set up an RDS MySQL Multi-AZ DB instance. Configure an appropriate backup window.
B. Set up an RDS MySQL Multi-AZ DB instance. Configure a read replica in a different Region.
C. Set up an RDS MySQL Single-AZ DB instance. Configure a read replica in a different Region.
D. Set up an RDS MySQL Single-AZ DB instance. Copy automated snapshots to at least one other Region.

Commented [LC322]: ANSWER

Question #384

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.
Which policy should be used to meet this requirement?

A. Simple routing policy
B. Latency routing policy
C. Multi-value routing policy
D. Geolocation routing policy

Commented [LC323]: ANSWER

Question #385

A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migration must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.
What should a solutions architect do to migrate and store the data at the LOWEST cost?

A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.
C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
D. Use AWS DataSync to transfer the data and deploy a DataSync agent on premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

Commented [LC324]: ANSWER

Question #386

A company is preparing to deploy a data lake on AWS. A solutions architect must define the encryption strategy tor data at rest m Amazon S3/ The company's security policy states:
➩ Keys must be rotated every 90 days.
➩ Strict separation of duties between key users and key administrators must be implemented.
➩ Auditing key usage must be possible.
What should the solutions architect recommend?

A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs)
B. Server-side encryption with AWS KMS managed keys (SSE-KMS) with AWS managed customer master keys (CMKs)
C. Server-side encryption with Amazon S3 managed keys (SSE-S3) with customer managed customer master keys (CMKs)
D. Server-side encryption with Amazon S3 managed keys (SSE-S3) with AWS managed customer master keys (CMKs)

Commented [LC325]: https://docs.aws.amazon.com/whitepapers/latest/kms-best-practices/aws-managed-and-customer-managed-cmks.html

Question #387

A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days.
Which storage solution is MOST cost-effective?

A. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Glacier 30 days from object creation. Delete the files 4 years after object creation.
B. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days from object creation. Delete the files 4 years after object creation.
C. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Delete the files 4 years after object creation.
D. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Move the files to S3 Glacier 4 years after object creation.

Commented [LC326]: Since they want that immediate access is always required I'd say C. B would be cheaper but still we need to make sure that in case of one AZ is down the file is still immediately accessed. It's a bad formulated question. Let's hope they don't put it in the test…

Question #388

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.
Which solution provides the LOWEST data transfer egress cost for the company?

A. Host the visualization tool on premises and query the data warehouse directly over the internet.
B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a DirectConnect connection at a location in the same Region.

Commented [LC327]: A,B wrong because we have already Direct Connect. C,D feasible but the least egress cost would be D.

Question #389

A mobile gaming company runs application servers on Amazon EC2 instances. The servers receive updates from players every 15 minutes. The mobile game creates a JSON object of the progress made in the game since the last update, and sends the JSON object to an Application Load Balancer. As the mobile game is played, game updates are being lost. The company wants to create a durable way to get the updates in order.
What should a solutions architect recommend to decouple the system?

A. Use Amazon Kinesis Data Streams to capture the data and store the JSON object in Amazon S3.
B. Use Amazon Kinesis Data Firehose to capture the data and store the JSON object in Amazon S3.
C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to capture the data and EC2 instances to process the messages in the queue.
D. Use Amazon Simple Notification Service (Amazon SNS) to capture the data and EC2 instances to process the messages sent to the Application Load Balancer.

Commented [LC328]: ANSWER

Question #390

A company has an application that runs on Amazon EC2 instances within a private subnet in a VPC. The instances access data in an Amazon S3 bucket in the same AWS Region. The VPC contains a NAT gateway in a public subnet to access the S3 bucket. The company wants to reduce costs by replacing the NAT gateway without compromising security or redundancy.
Which solution meets these requirements?

A. Replace the NAT gateway with a NAT instance.
B. Replace the NAT gateway with an internet gateway.
C. Replace the NAT gateway with a gateway VPC endpoint.
D. Replace the NAT gateway with an AWS Direct Connect connection.

Commented [LC329]: ANSWER

Question #391

A company hosts a website on premises and wants to migrate it to the AWS Cloud. The website exposes a single hostname to the internet but it routes its functions to different on-premises server groups based on the path of the URL. The server groups are scaled independently depending on the needs of the functions they support. The company has an AWS Direct Connect connection configured to its on-premises network.
What should a solutions architect do to provide path-based routing to send the traffic to the correct group of servers?

A. Route all traffic to an internet gateway. Configure pattern matching rules at the internet gateway to route traffic to the group of servers supporting that path.
B. Route all traffic to a Network Load Balancer (NLB) with target groups for each group of servers. Use pattern matching rules at the NLB to route traffic to the correct target group.
C. Route all traffic to an Application Load Balancer (ALB). Configure path-based routing at the ALB to route traffic to the correct target group for the servers supporting that path.
D. Use Amazon Route 53 as the DNS server. Configure Route 53 path-based alias records to route traffic to the correct Elastic Load Balancer for the group of servers supporting that path.

Commented [LC330]: ALB supports path-based routing and now on-premise resources. I'd say C.

Question #392

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

A. Enable storage auto scaling in RDS.
B. Increase the RDS database instance size.
C. Change the RDS database instance storage type to Provisioned IOPS.
D. Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance.

Commented [LC331]: B is cool but A is cooler.

Question #393

An ecommerce website is deploying its web application as Amazon Elastic Container Service (Amazon ECS) container instances behind an Application Load Balancer (ALB). During periods of high activity, the website slows down and availability is reduced. A solutions architect uses Amazon CloudWatch alarms to receive notifications whenever there is an availability issue so they can scale out resources. Company management wants a solution that automatically responds to such events.
Which solution meets these requirements?

A. Set up AWS Auto Scaling to scale out the ECS service when there are timeouts on the ALB. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
B. Set up AWS Auto Scaling to scale out the ECS service when the ALB CPU utilization is too high. Setup AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
C. Set up AWS Auto Scaling to scale out the ECS service when the service's CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
D. Set up AWS Auto Scaling to scale out the ECS service when the ALB target group CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

Commented [LC332]: ANSWER

Question #394

A company has a website deployed on AWS. The database backend is hosted on Amazon RDS for MySQL with a primary instance and five read replicas to support scaling needs. The read replicas should lag no more than 1 second behind the primary instance to support the user experience. As traffic on the website continues to increase, the replicas are falling further behind during periods of peak load, resulting in complaints from users when searches yield inconsistent results. A solutions architect needs to reduce the replication lag as much as possible, with minimal changes to the application code or operational requirements.
Which solution meets these requirements?

A. Migrate the database to Amazon Aurora MySQL. Replace the MySQL read replicas with Aurora Replicas and enable Aurora Auto Scaling
B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the website to check the cache before querying the database read endpoints.
C. Migrate the database from Amazon RDS to MySQL running on Amazon EC2 compute instances. Choose very large compute optimized instances for all replica nodes.
D. Migrate the database to Amazon DynamoDB. Initially provision a large number of read capacity units (RCUs) to support the required throughput with on- demand capacity scaling enabled.

Commented [LC333]: ANSWER

Question #395

A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels. The company has been experiencing application interruptions several times each day, resulting in lost transactions.
What should a solutions architect recommend to improve application resiliency?

A. Modify the shipping application to write to a local database.
B. Modify the application APIs to run serverless using AWS Lambda
C. Configure Amazon API Gateway to call the EC2 inventory application APIs.
D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS).

Commented [LC334]: A is wrong. This question is tricky, because it's not clear if the problem is on-prem or on EC2.

Decoupling would help with lost transactions, because if the EC2 crashes, the message would be kept in the queue until it's processed by the application, so it would be more resilient.

Probably it's D

Question #396

A company has a three-tier environment on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB) then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier that makes database calls.
What should a solutions architect do to improve the security of data in transit to the web tier?

A. Configure a TLS listener and add the server certificate on the NLB.
B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.
C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.
D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS).

Commented [LC335]: Tricky question. The goal is to protect DATA IN TRANSIT, so B is out (and wrong because it's not possible to attach to a NLB), D is for Data at REST so wrong.

Ref:
https://wa.aws.amazon.com/wat.question.SEC_9.en.html

Question #397

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.
What should a solutions architect recommend to meet these requirements?

A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.
B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.
C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.
D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

Commented [LC336]: ANSWER

Question #398

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.
There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.
What should a solutions architect do to increase the application's performance?

A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.
B. Create an Amazon S3 bucket. Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.
C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.
D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

Commented [LC337]: ANSWER

Question #399

A web application must persist order data to Amazon S3 to support near-real time processing. A solutions architect needs to create an architecture that is both scalable and fault tolerant.
Which solutions meet these requirements? (Choose two.)

A. Write the order event to an Amazon DynamoDB table. Use DynamoDB Streams to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
B. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use the queue to trigger an AWS Lambda function that parsers the payload and writes the data to Amazon S3.
C. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use the SNS topic to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
D. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

Commented [LC338]: ANSWER

E. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

Question #400

A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions. To communicate with each other, the instances use the internet for connectivity. The security team wants to ensure that no communication between the instances happens over the internet.
What should a solutions architect do to accomplish this?

A. Create a NAT gateway and update the route table of the EC2 instances' subnet.
B. Create a VPC endpoint and update the route table of the EC2 instances' subnet.
C. Create a VPN connection and update the route table of the EC2 instances' subnet.
D. Create a VPC peering connection and update the route table of the EC2 instances' subnet.

Commented [LC339]: ANSWER

Questions from 401-499

Question #401

An online shopping application accesses an Amazon RDS Multi-AZ DB instance. Database performance is slowing down the application. After upgrading to the next-generation instance type, there was no significant performance improvement.
Analysis shows approximately 700 IOPS are sustained, common queries run for long durations and memory utilization is high.
Which application change should a solutions architect recommend to resolve these issues?

A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.
B. Separate the long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database is needed.
C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query the cluster first and query the database only if needed.
D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed.

Commented [LC340]: ANSWER

Question #402

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year.
Which solution meets these requirements and is the MOST operationally efficient?

A. Server-side encryption with customer-provided keys (SSE-C)
B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation
D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

Commented [LC341]: Automatic rotation is every year

Question #403

A company is preparing to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database. The database cannot be migrated to a different engine because SQL Server features are used in the application's NET code. The company wants to attain the greatest availability possible while minimizing operational and management overhead.
What should a solutions architect do to accomplish this?

A. Install SQL Server on Amazon EC2 in a Multi-AZ deployment.
B. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment.
C. Deploy the database on Amazon RDS for SQL Server with Multi-AZ Replicas.
D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment.

Commented [LC342]: ANSWER

Question #404

A company has an application running on Amazon EC2 instances in a private subnet. The application needs to store and retrieve data in Amazon S3. To reduce costs, the company wants to configure its AWS resources in a cost-effective manner.
How should the company accomplish this?

A. Deploy a NAT gateway to access the S3 buckets.
B. Deploy AWS Storage Gateway to access the S3 buckets.
C. Deploy an S3 gateway endpoint to access the S3 buckets.
D. Deploy an S3 interface endpoint to access the S3 buckets.

Commented [LC343]: ANSWER

Question #405

A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real time recommendations. The application has a fleet of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance. Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure. The solution must ensure that data analysts are writing SQL to analyse the data only. No data can be lost during the deployment.
What should a solutions architect recommend?

A. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.
B. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.
C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.
D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

Commented [LC344]: ANSWER

Question #406

A company runs an application that uses multiple Amazon EC2 instances to gather data from its users. The data is then processed and transferred to Amazon S3 for long-term storage. A review of the application shows that there were long periods of time when the EC2 instances were not being used. A solutions architect needs to design a solution that optimizes utilization and reduces costs.
Which solution meets these requirements?

A. Use Amazon EC2 in an Auto Scaling group with On-Demand instances.
B. Build the application to use Amazon Lightsail with On-Demand Instances.
C. Create an Amazon CloudWatch cron job to automatically stop the EC2 instances when there is no activity.
D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (Amazon SQS) and AWS Lambda.

Commented [LC345]: If possible, that's the best choice

Question #407

A company is using Site-to-Site VPN connections for secure connectivity to its AWS Cloud resources from on premises. Due to an increase in traffic across the VPN connections to the Amazon EC2 instances, users are experiencing slower VPN connectivity.
Which solution will improve the VPN throughput?

A. Implement multiple customer gateways for the same network to scale the throughput.
B. Use a transit gateway with equal cost multipath routing and add additional VPN tunnels.
C. Configure a virtual private gateway with equal cost multipath routing and multiple channels.
D. Increase the number of tunnels in the VPN configuration to scale the throughput beyond the default limit.

Commented [LC346]: ANSWER
REF: https://aws.amazon.com/it/blogs/networking-and-content-delivery/scaling-vpn-throughput-using-aws-transit-gateway/

Question #408

A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity developers noticed slowdowns related to the game's metadata load times. Performance metrics indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots replication and sub-millisecond response times.
What should the solutions architect recommend to solve these issues?

A. Migrate the database to Amazon Aurora with Aurora Replicas.
B. Migrate the database to Amazon DyramoDB with global tables.
C. Add an Amazon ElastiCache for Redis layer in front of the database.
D. Add an Amazon ElastiCache for Memcached layer in front of the database.

Commented [LC347]: ANSWER.

Ref: https://aws.amazon.com/it/elasticache/redis-vs-memcached/

Question #409

A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly. Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.
What should a solutions architect do to optimize costs?

A. Create an additional NAT gateway. Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic.
B. Create an internet gateway. Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic.
C. Create a VPC endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint.
D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

Commented [LC348]: ANSWER

Question #410

A company is deploying an application in three AWS Regions using an Application Load Balancer. Amazon Route 53 will be used to distribute traffic between these regions.
Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

A. Create an A record with a latency policy.
B. Create an A record with a geolocation policy.
C. Create a CNAME record with a failover policy.
D. Create a CNAME record with a geoproximity policy.

Commented [LC349]: ANSWER

Question #411

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service Customer Master Keys (AWS KMS CMKs). A solutions architect needs to design a solution that will ensure the required permissions are set correctly.
Which combination of actions accomplish this? (Choose two.)

A. Attach the kms:decrypt permission to the Lambda function's resource policy.
B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy.
C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.

Commented [LC350]: ANSWER

E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

Commented [LC351]: ANSWER

Question #412

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. To meet the migration date, minimal changes can be made.
What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 Standard bucket with access to the web server.
B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
C. Create an Amazon Elastic File System (Amazon EFS) volume and mount it on all web servers.
D. Configure Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volumes and mount them on all web servers.

Commented [LC352]: ANSWER

Question #413

A company that operates a web application on premises is preparing to launch a newer version of the application on AWS. The company needs to route requests to either the AWS-hosted or the on-premises-hosted application based on the URL query string. The on-premises application is not available from the internet, and a VPN connection is established between Amazon VPC and the company's data center. The company wants to use an Application Load Balancer (ALB) for this launch.
Which solution meets these requirements?

A. Use two ALBs: one for on-premises and one for the AWS resource. Add hosts to each target group of each ALB. Route with Amazon Route 53 based on the URL query string.
B. Use two ALBs: one for on-premises and one for the AWS resource. Add hosts to the target group of each ALB. Create a software router on an EC2 instance based on the URL query string.
C. Use one ALB with two target groups: one for the AWS resource and one for on premises. Add hosts to each target group of the ALB. Configure listener rules based on the URL query string.
D. Use one ALB with two AWS Auto Scaling groups: one for the AWS resource and one for on premises. Add hosts to each Auto Scaling group. Route with Amazon Route 53 based on the URL query string.

Commented [LC353]: ANSWER

Question #414

A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases. Only the Amazon EC2 instances running in the private subnets should be able to access a database.
Which solution meets these requirements?

A. Create a now route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.
B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.
C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.
D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

Commented [LC354]: ANSWER

Question #415

A disaster response team is using drones to collect images of recent storm damage. The response team's laptops lack the storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.
What should a solutions architect recommend?

A. Use AWS Snowball Edge devices to process and store the images.
B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images.
D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

Commented [LC355]: This is a real known case:

https://aws.amazon.com/it/blogs/storage/hurricane-dorian-disaster-response-in-the-bahamas-using-aws-snowball-edge/

Question #416

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before levelling off.
What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two.)

A. Configure storage Auto Scaling on the RDS for Oracle instance.
B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
C. Configure an alarm on the RDS for Oracle instance for low free storage space.
D. Configure the Auto Scaling group to use the average CPU as the scaling metric.

Commented [LC356]: ANSWER

Commented [LC357]: ANSWER

E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Question #417

An engineering team is developing and deploying AWS Lambda functions. The team needs to create roles and manage policies in AWS IAM to configure the permissions of the Lambda functions.
How should the permissions for the team be configured so they also adhere to the concept of least privilege?

A. Create an IAM role with a managed policy attached. Allow the engineering team and the Lambda functions to assume this role.
B. Create an IAM group for the engineering team with an IAMFullAccess policy attached. Add all the users from the team to this IAM group.
C. Create an execution role for the Lambda functions. Attach a managed policy that has permission boundaries specific to these Lambda functions.
D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions. Allow the engineering team to assume this role.

Commented [LC358]: ANSWER

Question #418

A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains over 10 million rows. The database has 2 TB of General Purpose SSD (gp2) storage. There are millions of updates against this data every day through the company's website. The company has noticed some operations are taking 10 seconds or longer and has determined that the database storage performance is the bottleneck.
Which solution addresses the performance issue?

A. Change the storage type to Provisioned IOPS SSD (io1).
B. Change the instance to a memory-optimized instance class.
C. Change the instance to a burstable performance DB instance class.
D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Commented [LC359]: ***General Purpose (SSD)*** storage is suitable for a broad range of database workloads. Provides baseline of 3 IOPS/GiB and ability to burst to 3,000 IOPS.

Provisioned IOPS (SSD) storage is suitable for I/O-intensive database workloads. Provides flexibility to provision I/O ranging from 1,000 to 80,000 IOPS.

Standard instance class
Standard instances provide a balance of compute, memory, and network resources, and is a good choice for many database workloads.

Memory optimized classes
Memory optimized instances accelerate performance for workloads that process large data sets in memory.

Burstable classes
Burstable performance instances provide a baseline level of CPU performance with the ability to burst above the baseline.

Question #419

A company has an Amazon S3 bucket that contains mission-critical data. The company wants to ensure this data is protected from accidental deletion. The data should still be accessible, and a user should be able to delete the data intentionally.
Which combination of steps should a solutions architect take to accomplish this? (Choose two.)

A. Enable versioning on the S3 bucket.
B. Enable MFA Delete on the S3 bucket.
C. Create a bucket policy on the S3 bucket.
D. Enable default encryption on the S3 bucket.
E. Create a lifecycle policy for the objects in the S3 bucket.

Commented [LC360]: ANSWER

Question #420

A company has an on-premises business application that generates hundreds of files each day. These files are stored on an SMB file share and require a low-latency connection to the application servers. A new company policy states all application-generated files must be copied to AWS. There is already a VPN connection to AWS.
The application development team does not have time to make the necessary code modifications to move the application to AWS.
Which service should a solutions architect recommend to allow the application to copy files to AWS?

A. Amazon Elastic File System (Amazon EFS)
B. Amazon FSx for Windows File Server
C. AWS Snowball
D. AWS Storage Gateway

Commented [LC361]: ANSWER

Question #421

A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.
Which combination of steps should a solutions architect take to accomplish this? (Choose two.)

A. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
B. Create a bucket policy to make the objects in the S3 bucket public.
C. Create a bucket policy that limits access to only the application tier running in the VPC.
D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.
E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

Commented [LC362]: ANSWER

Commented [LC363]: ANSWER

Question #422

A solutions architect plans to convert a company's monolithic web application into a multi-tier application. The company wants to avoid managing its own infrastructure. The minimum requirements for the web application are high availability, scalability, and regional low latency during peak hours. The solution should also store and retrieve data with millisecond latency using the application's API.
Which solution meets these requirements?

A. Use AWS Fargate to host the web application with backend Amazon RDS Multi-AZ DB instances.
B. Use Amazon API Gateway with an edge-optimized API endpoint, AWS Lambda for compute, and Amazon DynamoDB as the data store.
C. Use an Amazon Route 53 routing policy with geolocation that points to an Amazon S3 bucket with static website hosting and Amazon DynamoDB as the data store.
D. Use an Amazon CloudFront distribution that points to an Elastic Load Balancer with an Amazon EC2 Auto Scaling group, along with Amazon RDS Multi-AZ DB instances.

Commented [LC364]: ANSWER. C,D requires infrastructure management. B is wrong because LAMBDA doesn't work for hosting a web tier.

Question #423

A team has an application that detects new objects being uploaded into an Amazon S3 bucket. The uploads trigger AWS Lambda function to write object metadata into an Amazon DynamoDB table and an Amazon RDS for PostgreSQL database.
Which action should the team take to ensure high availability?

A. Enable Cross-Region Replication in the S3 bucket.
B. Create a Lambda function for each Availability Zone the application is deployed in.
C. Enable Multi-AZ on the RDS for PostgreSQL database.
D. Create a DynamoDB stream for the DynamoDB table.

Commented [LC365]: ANSWER

Question #424

A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data. The application cannot be modified to use any other communication protocols other than NFS for this purpose.
Which storage solution should a solutions architect recommend for use after the migration?

A. AWS DataSync
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon Elastic File System (Amazon EFS)
D. Amazon EMR File System (Amazon EMRFS)

Commented [LC366]: ANSWER

Question #425

An application calls a service run by a vendor. The vendor charges based on the number of calls. The finance department needs to know the number of calls that are made to the service to validate the billing statements.
How can a solutions architect design a system to durably store the number of calls without requiring changes to the application?

A. Call the service through an internet gateway.
B. Decouple the application from the service with an Amazon Simple Queue Service (Amazon SQS) queue.
C. Publish a custom Amazon CloudWatch metric that counts calls to the service.
D. Call the service through a VPC peering connection.

Commented [LC367]: ANSWER

Question #426

A company wants to reduce its Amazon S3 storage costs in its production environment without impacting durability or performance of the stored objects.
What is the FIRST step the company should take to meet these objectives?

A. Enable Amazon Macie on the business-critical S3 buckets to classify the sensitivity of the objects.
B. Enable S3 analytics to identify S3 buckets that are candidates for transitioning to S3 Standard-Infrequent Access (S3 Standard-IA).
C. Enable versioning on all business-critical S3 buckets.
D. Migrate the objects in all S3 buckets to S3 Intelligent-Tiering.

Commented [LC368]: ANSWER

Question #427

A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totalling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.
Which storage solution meets these requirements MOST cost-effectively?

A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon Elasticsearch Service (Amazon ES)
D. Amazon S3

Commented [LC369]: ANSWER

Question #428

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of the application and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.
Which solution meets these requirements?

A. Use AWS CloudTrail to generate a list of resources with the application tag.
B. Use the AWS CLI to query each service across all Regions to report the tagged components.
C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.
D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

Commented [LC370]: ANSWER

Question #429

A development team is deploying a new product on AWS and is using AWS Lambda as part of the deployment. The team allocates 512 MB of memory for one of the Lambda functions. With this memory allocation, the function is completed in 2 minutes. The function runs millions of times monthly, and the development team is concerned about cost. The team conducts tests to see how different Lambda memory allocations affect the cost of the function.
Which steps will reduce the Lambda costs for the product? (Choose two.)

A. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 1 minute.
B. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 90 seconds.
C. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 4 minutes.
D. Increase the memory allocation for this Lambda function to 2,048 MB if this change causes the execution time of each function to be less than 1 minute.
E. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 5 minutes.

Commented [LC371]: To explain this formally you can graph a x,y plane (time, capacity) and calculate the area of all the superficies fixing the axis for every point. You can calculate the area (which is the cost) by eyes and you see that the answers are the ones indicated. To do it quickly and without math, you can count the "square" of the areas.

If you have doubt contact me and I'll be happy to clarify.

You could also have a comparative approach. Since the cost is measured by runtime and capacity, it's safe to exclude B because A takes less time with the same capacity.

Inverting… D is safe to eliminate because A for the same runtime requires less capacity.

Between C and E, E is safe to eliminate because for the same capacity it requires runtime.

Commented [LC372]: ANSWER

Question #430

A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.
Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

Commented [LC373]: ANSWER

Question #431

A user owns a MySQL database that is accessed by various clients who expect, at most, 100 ms latency on requests. Once a record is stored in the database, it is rarely changed. Clients only access one record at a time.
Database access has been increasing exponentially due to increased client demand. The resultant load will soon exceed the capacity of the most expensive hardware available for purchase. The user wants to migrate to AWS, and is willing to change database systems.
Which service would alleviate the database load issue and offer virtually unlimited scalability for the future?

A. Amazon RDS
B. Amazon DynamoDB
C. Amazon Redshift
D. AWS Data Pipeline

Commented [LC374]: Since the user it's "willing to change db systems", the answer is B

Question #432

A company designs a mobile app for its customers to upload photos to a website. The app needs a secure login with multi-factor authentication (MFA). The company wants to limit the initial build time and the maintenance of the solution.
Which solution should a solutions architect recommend to meet these requirements?

A. Use Amazon Cognito Identity with SMS-based MFA.
B. Edit IAM policies to require MFA for all users.
C. Federate IAM against the corporate Active Directory that requires MFA.

Commented [LC375]: ANSWER

D. Use Amazon API Gateway and require server-side encryption (SSE) for photos.

Question #433

A company has an application that uses overnight digital images of products on store shelves to analyse inventory data. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) and obtains the images from an Amazon S3 bucket for its metadata to be processed by worker nodes for analysis. A solutions architect needs to ensure that every image is processed by the worker nodes.
What should the solutions architect do to meet this requirement in the MOST cost-efficient way?

A. Send the image metadata from the application directly to a second ALB for the worker nodes that use an Auto Scaling group of EC2 Spot Instances as the target group.
B. Process the image metadata by sending it directly to EC2 Reserved Instances in an Auto Scaling group. With a dynamic scaling policy, use an Amazon CloudWatch metric for average CPU utilization of the Auto Scaling group as soon as the front-end application obtains the images.
C. Write messages to Amazon Simple Queue Service (Amazon SQS) when the front-end application obtains an image. Process the images with EC2 On-Demand instances in an Auto Scaling group with instance scale-in protection and a fixed number of instances with periodic health checks.
D. Write messages to Amazon Simple Queue Service (Amazon SQS) when the application obtains an image. Process the images with EC2 Spot Instances in an Auto Scaling group with instance scale-in protection and a dynamic scaling policy using a custom Amazon CloudWatch metric for the current number of messages in the queue.

Commented [LC376]: D is fine even though it's Spot Instances because SQS visibility timeout. If the message is not consumed correctly (i.e. the spot instance terminates) the message goes back to the SQS, so it's sufficiently enough to guarantee that all messages are going to be processed.

Question #434

A solutions architect needs to host a high performance computing (HPC) workload in the AWS Cloud. The workload will run on hundreds of Amazon EC2 instances and will require parallel access to a shared file system to enable distributed processing of large datasets. Datasets will be accessed across multiple instances simultaneously. The workload requires access latency within 1 ms. After processing has completed, engineers will need access to the dataset for manual postprocessing.
Which solution will meet these requirements?

A. Use Amazon Elastic File System (Amazon EFS) as a shared file system. Access the dataset from Amazon EFS.
B. Mount an Amazon S3 bucket to serve as the shared file system. Perform postprocessing directly from the S3 bucket.
C. Use Amazon FSx for Lustre as a shared file system. Link the file system to an Amazon S3 bucket for postprocessing.
D. Configure AWS Resource Access Manager to share an Amazon S3 bucket so that it can be mounted to all instances for processing and postprocessing.

Commented [LC377]: ANSWER

Question #435

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.
What should a solutions architect do to meet these requirements?

A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

Commented [LC378]: ANSWER

Question #436

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.
Which solution meets these requirements?

A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Commented [LC379]: ANSWER

Question #437

A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.
The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure.
Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.
What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon Elasticsearch Service (Amazon ES) cluster. Set up the Amazon ES cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days.
D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts, and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

Commented [LC380]: ANSWER

Question #438

A company has two AWS accounts: Production and Development. There are code changes ready in the Development account to push to the Production account.
In the alpha phase, only two senior developers on the development team need access to the Production account. In the beta phase, more developers might need access to perform testing as well.
What should a solutions architect recommend?

A. Create two policy documents using the AWS Management Console in each account. Assign the policy to developers who need access.
B. Create an IAM role in the Development account. Give one IAM role access to the Production account. Allow developers to assume the role.
C. Create an IAM role in the Production account with the trust policy that specifies the Development account. Allow developers to assume the role.
D. Create an IAM group in the Production account and add it as a principal in the trust policy that specifies the Production account. Add developers to the group.

Commented [LC381]: ANSWER

Question #439

A company is using an Amazon S3 bucket to store data uploaded by different departments from multiple locations. During an AWS Well-Architected review, the financial manager notices that 10 TB of S3 Standard storage data has been charged each month. However, in the AWS Management Console for Amazon S3, using the command to select all files and folders shows a total size of 5 TB.
What are the possible causes for this difference? (Choose two.)

A. Some files are stored with deduplication.
B. The S3 bucket has versioning enabled.
C. There are incomplete S3 multipart uploads.
D. The S3 bucker has AWS Key Management Service (AWS KMS) enabled.
E. The S3 bucket has Intelligent-Tiering enabled.

Commented [LC382]: ANSWER

Question #440

A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.
Which solution meets these requirements?

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.
D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

Commented [LC383]: Ref https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html

Question #441

A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.
The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.
What should a solutions architect do to meet these requirements?

A. Enable HTTP health checks on the NLB, supplying the URL of the company's application.
B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.
C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.
D. Create an Amazon CloudWatch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Commented [LC384]: ANSWER

Question #442

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.
What is the MOST cost-effective solution to connect these VPCs?

A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Commented [LC385]: ANSWER

Question #443

A company is deploying an application that processes streaming data in near-real time. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to provide the lowest possible latency between nodes.
Which combination of network solutions will meet these requirements? (Choose two.)

A. Enable and configure enhanced networking on each EC2 instance.
B. Group the EC2 instances in separate accounts.
C. Run the EC2 instances in a cluster placement group.
D. Attach multiple elastic network interfaces to each EC2 instance.
E. Use Amazon Elastic Block Store (Amazon EBS) optimized instance types.

Commented [LC386]: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

Commented [LC387]: ANSWER

Question #444

A company is running a global application. The application's users submit multiple videos that are then merged into a single video file. The application uses a single Amazon S3 bucket in the us-east-1 Region to receive uploads from users. The same S3 bucket provides the download location of the single video file that is produced. The final video file output has an average size of 250 GB.
The company needs to develop a solution that delivers faster uploads and downloads of the video files that are stored in Amazon S3. The company will offer the solution as a subscription to users who want to pay for the increased speed.
What should a solutions architect do to meet these requirements?

A. Enable AWS Global Accelerator for the S3 endpoint. Adjust the application's upload and download links to use the Global Accelerator S3 endpoint for users who have a subscription.
B. Enable S3 Cross-Region Replication to S3 buckets in all other AWS Regions. Use an Amazon Route 53 geolocation routing policy to route S3 requests based on the location of users who have a subscription.
C. Create an Amazon CloudFront distribution and use the S3 bucket in us-east-1 as an origin. Adjust the application to use the CloudFront URL as the upload and download links for users who have a subscription.
D. Enable S3 Transfer Acceleration for the S3 bucket in us-east-1. Configure the application to use the bucket's S3-accelerate endpoint domain name for the upload and download links for users who have a subscription.

Commented [LC388]: ANSWER

Question #445

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
            "Sid": "1",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                 "StringEquals": {
                      "ec2:Region": "us-east-1"
                 }
            }
       },
       {
            "Sid": "2",
            "Effect": "Deny",
            "Action": [
                 "ec2:StopInstances",
                 "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                 "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
     ]
  }
```

What are the effective IAM permissions of this policy for group members?

A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.
D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Commented [LC389]: ANSWER

Question #446

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.
What should a solutions architect do to mitigate any single point of failure in this architecture?

A. Add a set of VPNs between the Management and Production VPCs.
B. Add a second virtual private gateway and attach it to the Management VPC.
C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Commented [LC390]: ANSWER

Question #447

A company is using AWS Organizations with two AWS accounts: Logistics and Sales. The Logistics account operates an Amazon Redshift cluster. The Sales account includes Amazon EC2 instances. The Sales account needs to access the Logistics account's Amazon Redshift cluster.
What should a solutions architect recommend to meet this requirement MOST cost-effectively?

A. Set up VPC sharing with the Logistics account as the owner and the Sales account as the participant to transfer the data.
B. Create an AWS Lambda function in the Logistics account to transfer data to the Amazon EC2 instances in the Sales account.
C. Create a snapshot of the Amazon Redshift cluster, and share the snapshot with the Sales account. In the Sales account, restore the cluster by using the snapshot ID that is shared by the Logistics account.
D. Run COPY commands to load data from Amazon Redshift into Amazon S3 buckets in the Logistics account. Grant permissions to the Sales account to access the S3 buckets of the Logistics account.

Commented [LC391]: ANSWER

Question #448

A company is using Amazon Redshift for analytics and to generate customer reports. The company recently acquired 50 TB of additional customer demographic data. The data is stored in .csv files in Amazon S3. The company needs a solution that joins the data and visualizes the results with the least possible cost and effort.
What should a solutions architect recommend to meet these requirements?

A. Use Amazon Redshift Spectrum to query the data in Amazon S3 directly and join that data with the existing data in Amazon Redshift. Use Amazon QuickSight to build the visualizations.
B. Use Amazon Athena to query the data in Amazon S3. Use Amazon QuickSight to join the data from Athena with the existing data in Amazon Redshift and to build the visualizations.
C. Increase the size of the Amazon Redshift cluster, and load the data from Amazon S3. Use Amazon EMR Notebooks to query the data and build the visualizations in Amazon Redshift.
D. Export the data from the Amazon Redshift cluster into Apache Parquet files in Amazon S3. Use Amazon Elasticsearch Service (Amazon ES) to query the data. Use Kibana to visualize the results.

Commented [LC392]: https://docs.aws.amazon.com/redshift/latest/dg/c-getting-started-using-spectrum.html

Question #449

A solutions architect must provide a fully managed replacement for an on-premises solution that allows employees and partners to exchange files. The solution must be easily accessible to employees connecting from on-premises systems, remote employees, and external partners.
Which solution meets these requirements?

A. Use AWS Transfer for SFTP to transfer files into and out of Amazon S3.
B. Use AWS Snowball Edge for local storage and large-scale data transfers.
C. Use Amazon FSx to store and transfer files to make them available remotely.
D. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.

Commented [LC393]: ANSWER

Question #450

A company's database is hosted on an Amazon Aurora MySQL DB cluster in the us-east-1 Region. The database is 4 TB in size. The company needs to expand its disaster recovery strategy to the us-west-2 Region. The company must have the ability to failover to us-west-2 with a recovery time objective (RTO) of 15 minutes.
What should a solutions architect recommend to meet these requirements?

A. Create a Multi-Region Aurora MySQL DB cluster in us-east-1 and us-west-2. Use an Amazon Route 53 health check to monitor us-east-1 and fail over to us-west-2 upon failure.
B. Take a snapshot of the DB cluster in us-east-1. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to copy the snapshot to us-west-2 and restore the snapshot in us-west-2 when failure is detected.
C. Create an AWS CloudFormation script to create another Aurora MySQL DB cluster in us-west-2 in case of failure. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to deploy the AWS CloudFormation stack in us-west-2 when failure is detected.
D. Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to promote the DB cluster in us-west-2 when failure is detected.

Commented [LC394]: ANSWER

Question #451

A company is migrating its applications to AWS. Currently, applications that run on premises generate hundreds of terabytes of data that is stored on a shared file system. The company is running an analytics application in the cloud that runs hourly to generate insights from this data.
The company needs a solution to handle the ongoing data transfer between the on-premises shared file system and Amazon S3. The solution also must be able to handle occasional interruptions in internet connectivity.
Which solutions should the company use for the data transfer to meet these requirements?

A. AWS DataSync
B. AWS Migration Hub
C. AWS Snowball Edge Storage Optimized
D. AWS Transfer for SFTP

Commented [LC395]: B is wrong. C is wrong because it's only on-going. D is wrong because doesn't support occasional interruptions

Question #452

A solutions architect is designing the architecture for a new web application. The application will run on AWS Fargate containers with an Application Load Balancer (ALB) and an Amazon Aurora PostgreSQL database. The web application will perform primarily read queries against the database.
What should the solutions architect do to ensure that the website can scale with increasing traffic? (Choose two.)

A. Enable auto scaling on the ALB to scale the load balancer horizontally.
B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.
C. Enable cross-zone load balancing on the ALB to distribute the load evenly across containers in all Availability Zones.
D. Configure an Amazon Elastic Container Service (Amazon ECS) cluster in each Availability Zone to distribute the load across multiple Availability Zones.

Commented [LC396]: ANSWER

E. Configure Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling with a target tracking scaling policy that is based on CPU utilization.

Commented [LC397]: ANSWER

Question #453

A company captures ordered clickstream data from multiple websites and uses batch processing to analyse the data. The company receives 100 million event records, all approximately 1 KB in size, each day. The company loads the data into Amazon Redshift each night, and business analysts consume the data.
The company wants to move toward near-real-time data processing for timely insights. The solution should process the streaming data while requiring the least possible operational overhead.
Which combination of AWS services will meet these requirements MOST cost-effectively? (Choose two.)

A. Amazon EC2
B. AWS Batch
C. Amazon Simple Queue Service (Amazon SQS)
D. Amazon Kinesis Data Firehose
E. Amazon Kinesis Data Analytics

Commented [LC398]: ANSWER

Question #454

A company has a customer relationship management (CRM) application that stores data in an Amazon RDS DB instance that runs Microsoft SQL Server. The company's IT staff has administrative access to the database. The database contains sensitive data. The company wants to ensure that the data is not accessible to the IT staff and that only authorized personnel can view the data.
What should a solutions architect do to secure the data?

A. Use client-side encryption with an Amazon RDS managed key.
B. Use client-side encryption with an AWS Key Management Service (AWS KMS) customer managed key.
C. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) default encryption key.
D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

Commented [LC399]: ANSWER

Question #455

A company with a single AWS account runs its internet-facing containerized web application on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.
The EKS cluster is placed in a private subnet of a VPC. System administrators access the EKS cluster through a bastion host on a public subnet.
A new corporate security policy requires the company to avoid the use of bastion hosts. The company also must not allow internet connectivity to the EKS cluster.
Which solution meets these requirements MOST cost-effectively?

A. Set up an AWS Direct Connect connection.
B. Create a transit gateway.
C. Establish a VPN connection.
D. Use AWS Storage Gateway.

Commented [LC400]: ANSWER

Question #456

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.
The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.
What should a solutions architect do to improve the performance of the data tier?

A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
B. Migrate from Amazon RDS to Amazon Elasticsearch Service (Amazon ES) with Kibana.
C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.
D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

Commented [LC401]: Even though it doesn't speak about common or frequent data, the only feasible is D.

Question #457

A company is migrating a large, mission-critical database to AWS. A solutions architect has decided to use an Amazon RDS for MySQL Multi-AZ DB instance that is deployed with 80,000 Provisioned IOPS for storage. The solutions architect is using AWS Database Migration Service (AWS DMS) to perform the data migration. The migration is taking longer than expected, and the company wants to speed up the process. The company's network team has ruled out bandwidth as a limiting factor.
Which actions should the solutions architect take to speed up the migration? (Choose two.)

A. Disable Multi-AZ on the target DB instance.
B. Create a new DMS instance that has a larger instance size.
C. Turn off logging on the target DB instance until the initial load is complete.
D. Restart the DMS task on a new DMS instance with transfer acceleration enabled.
E. Change the storage type on the target DB instance to Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2).

Commented [LC402]: This is really tricky. The ref says that A is correct and also that C is correct IN CASE you're not migrating to RDS. In this case, the migration is to RDS. So, A and B are the answers.

Ref:
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_BestPractices.html

Question #458

A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.
What should a solutions architect do to meet these requirements?

A. Use Amazon EC2 instances, and install Docker on the instances.
B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.
C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

Commented [LC403]: ANSWER

Question #459

A company is designing a new application that runs in a VPC on Amazon EC2 instances. The application stores data in Amazon S3 and uses Amazon DynamoDB as its database. For compliance reasons, the company prohibits all traffic between the EC2 instances and other AWS services from passing over the public internet.
What can a solutions architect do to meet this requirement?

A. Configure gateway VPC endpoints to Amazon S3 and DynamoDB.
B. Configure interface VPC endpoints to Amazon S3 and DynamoDB.
C. Configure a gateway VPC endpoint to Amazon S3. Configure an interface VPC endpoint to DynamoDB.
D. Configure a gateway VPC endpoint to DynamoDB. Configure an interface VPC endpoint to Amazon S3.

Commented [LC404]: ANSWER

Question #460

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.
What should a solutions architect do to meet these requirements when configuring the logs?

A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.
B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Commented [LC405]: ANSWER

Question #461

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.
The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.
Which solution will meet these requirements?

A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS Single Sign-On.

Commented [LC406]: ANSWER

Question #462

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.
What should a solutions architect do to meet this requirement with the LEAST operational effort?

A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.
B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.
C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.
D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket.

Commented [LC407]: ANSWER

Question #463

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.
B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.
C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.
D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.
E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Commented [LC408]: ANSWER

Commented [LC409]: ANSWER

Question #464

A company recently launched a new service that involves medical images. The company scans the images and sends them from its on-premises data center through an AWS Direct Connect connection to Amazon EC2 instances. After processing is complete, the images are stored in an Amazon S3 bucket.

A company requirement states that the EC2 instances cannot be accessible through the internet. The EC2 instances run in a private subnet, which has a default route back to the on-premises data center for outbound internet access.

Usage of the new service is increasing rapidly. A solutions architect must recommend a solution that meets the company's requirements and reduces the Direct Connect charges.

Which solution accomplishes these goals MOST cost-effectively?

A. Configure a VPC endpoint for Amazon S3. Add an entry to the private subnet's route table for the S3 endpoint.
B. Configure a NAT gateway in a public subnet. Configure the private subnet's route table to use the NAT gateway.
C. Configure Amazon S3 as a file system mount point on the EC2 instances. Access Amazon S3 through the mount.
D. Move the EC2 instances into a public subnet. Configure the public subnet route table to point to an internet gateway.

Commented [LC410]: ANSWER

Question #465

A company is building an online multiplayer game. The game communicates by using UDP, and low latency between the client and the backend is important. The backend is hosted on Amazon EC2 instances that can be deployed to multiple AWS Regions to meet demand. The company needs the game to be highly available so that users around the world can access the game at all times.

What should a solutions architect do to meet these requirements?

A. Deploy Amazon CloudFront to support the global traffic. Configure CloudFront with an origin group to allow access to EC2 instances in multiple Regions.
B. Deploy an Application Load Balancer in one Region to distribute traffic to EC2 instances in each Region that hosts the game's backend instances.
C. Deploy Amazon CloudFront to support an origin access identity (OAI). Associate the OAI with EC2 instances in each Region to support global traffic.
D. Deploy a Network Load Balancer in each Region to distribute the traffic. Use AWS Global Accelerator to route traffic to the correct Regional endpoint.

Commented [LC411]: ANSWER

Question #466

A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.

Which combination of configuration options will meet these requirements? (Choose two.)

A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Commented [LC412]: A is correct because the EC2 instances are in the private subnets. Hence C is wrong. E is also correct.

Commented [LC413]: ANSWER

Question #467

A security team needs to enforce the rotation of all IAM users' access keys every 90 days. If an access key is found to be older, the key must be made inactive and removed. A solutions architect must create a solution that will check for and remediate any keys older than 90 days.
Which solution meets these requirements with the LEAST operational effort?

A. Create an AWS Config rule to check for the key age. Configure the AWS Config rule to run an AWS Batch job to remove the key.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Configure the rule to run an AWS Batch job to remove the key.
C. Create an AWS Config rule to check for the key age. Define an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule an AWS Lambda function to remove the key.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Define an EventBridge (CloudWatch Events) rule to run an AWS Batch job to remove the key.

Commented [LC414]: ANSWER

Question #468

A solutions architect must provide an automated solution for a company's compliance policy that states security groups cannot include a rule that allows SSH from 0.0.0.0/0. The company needs to be notified if there is any breach in the policy. A solution is needed as soon as possible.
What should the solutions architect do to meet these requirements with the LEAST operational overhead?

A. Write an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses and creates a notification every time it finds one.
B. Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.
C. Create an IAM role with permissions to globally open security groups and network ACLs. Create an Amazon Simple Notification Service (Amazon SNS) topic to generate a notification every time the role is assumed by a user.
D. Configure a service control policy (SCP) that prevents non-administrative users from creating or editing security groups. Create a notification in the ticketing system when a user requests a rule that needs administrator permissions.

Commented [LC415]: ANSWER

Question #469

A media company is using two video conversion tools that run on Amazon EC2 instances. One tool runs on Windows instances, and the other tool runs on Linux instances. Each video file is large in size and must be processed by both tools.
The company needs a storage solution that can provide a centralized file system that can be mounted on all the EC2 instances that are used in this process.
Which solution meets these requirements?

A. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances.
B. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket.
C. Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances
D. Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances.

Commented [LC416]: ANSWER

Question #470

A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet.
An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets.
Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.
What should the solutions architect recommend to meet this requirement?

A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.
B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.
C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.
D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

Commented [LC417]: You can't deny in security groups. You do that at L4 and with ACL at the subnets level.

Question #471

A company is planning to migrate a TCP-based application into the company's VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company's data center. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS.
What should a solutions architect recommend to meet this requirement?

A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

Commented [LC418]: ANSWER

Question #472

An ecommerce company is creating an application that requires a connection to a third-party payment service to process payments. The payment service needs to explicitly allow the public IP address of the server that is making the payment request. However, the company's security policies do not allow any server to be exposed directly to the public internet.
Which solution will meet these requirements?

A. Provision an Elastic IP address. Host the application servers on Amazon EC2 instances in a private subnet. Assign the public IP address to the application servers.
B. Create a NAT gateway in a public subnet. Host the application servers on Amazon EC2 instances in a private subnet. Route payment requests through the NAT gateway.
C. Deploy an Application Load Balancer (ALB). Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the ALB.
D. Set up an AWS Client VPN connection to the payment service. Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the VPN.

Commented [LC419]: ANSWER

Question #473

A company is running an ASP.NET MVC application on a single Amazon EC2 instance. A recent increase in application traffic is causing slow response times for users during lunch hours. The company needs to resolve this concern with the least amount of configuration.
What should a solutions architect recommend to meet these requirements?

A. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling and time-based scaling to handle scaling during lunch hours.
B. Move the application to Amazon Elastic Container Service (Amazon ECS). Create an AWS Lambda function to handle scaling during lunch hours.
C. Move the application to Amazon Elastic Container Service (Amazon ECS). Configure scheduled scaling for AWS Application Auto Scaling during lunch hours.
D. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling, and create an AWS Lambda function to handle scaling during lunch hours.

Commented [LC420]: ANSWER.

Ref. https://docs.aws.amazon.com/toolkit-for-visual-studio/latest/user-guide/deployment-beanstalk-traditional.html

Question #474

An online gaming company is designing a game that is expected to be popular all over the world. A solutions architect needs to define an AWS Cloud architecture that supports near-real-time recording and displaying of current game statistics for each player, along with the names of the top 25 players in the world, at any given time.
Which AWS database solution and configuration should the solutions architect use to meet these requirements?

A. Use Amazon RDS for MySQL as the data store for player activity. Configure the RDS DB instance for Multi-AZ support.
B. Use Amazon DynamoDB as the data store for player activity. Configure DynamoDB Accelerator (DAX) for the player data.
C. Use Amazon DynamoDB as the data store for player activity. Configure global tables in each required AWS Region for the player data.
D. Use Amazon RDS for MySQL as the data store for player activity. Configure cross-Region read replicas in each required AWS Region based on player proximity.

Commented [LC421]: ANSWER

Question #475

A company uses Amazon RDS for PostgreSQL databases for its data tier. The company must implement password rotation for the databases.
Which solution meets this requirement with the LEAST operational overhead?

A. Store the password in AWS Secrets Manager. Enable automatic rotation on the secret.
B. Store the password in AWS Systems Manager Parameter Store. Enable automatic rotation on the parameter.
C. Store the password in AWS Systems Manager Parameter Store. Write an AWS Lambda function that rotates the password.
D. Store the password in AWS Key Management Service (AWS KMS). Enable automatic rotation on the customer master key (CMK).

Commented [LC422]: ANSWER

Question #476

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.
A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyse.
Which system architecture should the solutions architect recommend?

A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.
B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.
C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Commented [LC423]: ANSWER

Question #477

An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.
What should a solutions architect do to meet these requirements?

A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.
B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.
C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.
D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Commented [LC424]: ANSWER

Question #478

A company has been running a web application with an Oracle relational database in an on-premises data center for the past 15 years. The company must migrate the database to AWS. The company needs to reduce operational overhead without having to modify the application's code.
Which solution meets these requirements?

A. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon RDS.
B. Use Amazon EC2 instances to migrate and operate the database servers.
C. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon DynamoDB.
D. Use an AWS Snowball Edge Storage Optimized device to migrate the data from Oracle to Amazon Aurora.

Commented [LC425]: ANSWER

Question #479

A company is running an application on Amazon EC2 instances. Traffic to the workload increases substantially during business hours and decreases afterward.
The CPU utilization of an EC2 instance is a strong indicator of end-user demand on the application. The company has configured an Auto Scaling group to have a minimum group size of 2 EC2 instances and a maximum group size of 10 EC2 instances.
The company is concerned that the current scaling policy that is associated with the Auto Scaling group might not be correct. The company must avoid over-provisioning EC2 instances and incurring unnecessary costs.
What should a solutions architect recommend to meet these requirements?

A. Configure Amazon EC2 Auto Scaling to use a scheduled scaling plan and launch an additional 8 EC2 instances during business hours.
B. Configure AWS Auto Scaling to use a scaling plan that enables predictive scaling. Configure predictive scaling with a scaling mode of forecast and scale, and to enforce the maximum capacity setting during scaling.
C. Configure a step scaling policy to add 4 EC2 instances at 50% CPU utilization and add another 4 EC2 instances at 90% CPU utilization. Configure scale-in policies to perform the reverse and remove EC2 instances based on the two values.
D. Configure AWS Auto Scaling to have a desired capacity of 5 EC2 instances, and disable any existing scaling policies. Monitor the CPU utilization metric for 1 week. Then create dynamic scaling policies that are based on the observed values.

Commented [LC426]: ANSWER

Question #480

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.
Which feature should the solutions architect include in the design to meet this requirement?

A. Read replicas
B. Manual snapshots
C. Automated backups
D. Multi-AZ deployments

Commented [LC427]: ANSWER

Question #482

A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.
What should a solutions architect do to meet this requirement?

A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer.
B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region.
C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application.
D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer.

Commented [LC428]: ANSWER

Question #483

A company is relocating its data center and wants to securely transfer 50 TB of data to AWS within 2 weeks. The existing data center has a Site-to-Site VPN connection to AWS that is 90% utilized.
Which AWS service should a solutions architect use to meet these requirements?

A. AWS DataSync with a VPC endpoint
B. AWS Direct Connect
C. AWS Snowball Edge Storage Optimized
D. AWS Storage Gateway

Commented [LC429]: ANSWER

Question #484

An entertainment company is using Amazon DynamoDB to store media metadata. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.
What should a solutions architect recommend to meet this requirement?

A. Use Amazon ElastiCache for Redis.
B. Use Amazon DynamoDB Accelerator (DAX).
C. Replicate data by using DynamoDB global tables.
D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Commented [LC430]: ANSWER

Question #485

A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications.
What should a solutions architect do to reduce the operational burden?

A. Use multi-factor authentication (MFA) to protect the encryption keys.
B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys.
C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.
D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.

Commented [LC431]: ANSWER

Question #486

A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.
Which solution meets these requirements with the LEAST amount of operational overhead?

A. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.
D. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

Commented [LC432]: ANSWER

Question #487

A company runs an application in the AWS Cloud and uses Amazon DynamoDB as the database. The company deploys Amazon EC2 instances to a private network to process data from the database. The company uses two NAT instances to provide connectivity to DynamoDB.
The company wants to retire the NAT instances. A solutions architect must implement a solution that provides connectivity to DynamoDB and that does not require ongoing management.
What is the MOST cost-effective solution that meets these requirements?

A. Create a gateway VPC endpoint to provide connectivity to DynamoDB.
B. Configure a managed NAT gateway to provide connectivity to DynamoDB.
C. Establish an AWS Direct Connect connection between the private network and DynamoDB.
D. Deploy an AWS PrivateLink endpoint service between the private network and DynamoDB.

Commented [LC433]: ANSWER

Question #488

A solutions architect is designing a two-tiered architecture that has separate private subnets for compute resources and the database. An AWS Lambda function that is deployed in the compute subnets needs connectivity to the database.
Which solution will provide this connectivity in the MOST secure way?

A. Configure the Lambda function to use Amazon RDS Proxy outside the VPC.
B. Associate a security group with the Lambda function. Authorize this security group in the database's security group.
C. Authorize the compute subnet's CIDR ranges in the database's security group.
D. During the initialization phase, authorize all IP addresses in the database's security group temporarily. Remove the rule after the initialization is complete.

Commented [LC434]: ANSWER

Question #489

A ride-sharing company stores historical service usage data as structured .csv data files in Amazon S3. A data analyst needs to perform SQL queries on this data.
A solutions architect must recommend a solution that optimizes cost-effectiveness for the queries.
Which solution meets these requirements?

A. Create an Amazon EMR cluster. Load the data. Perform the queries.
B. Create an Amazon Redshift cluster. Import the data. Perform the queries.
C. Create an Amazon Aurora PostgreSQL DB cluster. Import the data. Perform the queries.
D. Create an Amazon Athena database. Associate the data in Amazon S3. Perform the queries.

Commented [LC435]: ANSWER

Question #490

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets.
Which steps should a solutions architect take to block requests from unauthorized users? (Choose two.)

A. Create a usage plan with an API key that is shared with genuine users only.
B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.
C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.
D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.
E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

Commented [LC436]: ANSWER

Question #491

A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.
An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.
What should the solutions architect do to maximize reliability of the application's infrastructure?

A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.
B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.
C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.
D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On- Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances. Update the DB instance to be Multi-AZ, and enable deletion protection.

Commented [LC437]: ANSWER

Question #492

An online photo-sharing company stores its photos in an Amazon S3 bucket that exists in the us-west-1 Region. The company needs to store a copy of all existing and new photos in another geographical location.
Which solution will meet this requirement with the LEAST operational effort?

A. Create a second S3 bucket in us-east-1. Enable S3 Cross-Region Replication from the existing S3 bucket to the second S3 bucket.
B. Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.
C. Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle management rule to save photos into the second S3 bucket.
D. Create a second S3 bucket in us-east-1 to store the replicated photos. Configure S3 event notifications on object creation and update events that invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Commented [LC438]: This is not enough actually. You need to contact the AWS Support and open a case to replicate EXISTING objects. So this answer may be wrong.

Question #493

A company wants to migrate its accounting system from an on-premises data center to the AWS Cloud in a single AWS Region. Data security and an immutable audit log are the top priorities. The company must monitor all AWS activities for compliance auditing. The company has enabled AWS CloudTrail but wants to make sure it meets these requirements.
Which actions should a solutions architect take to protect and secure CloudTrail? (Choose two.)

A. Enable CloudTrail log file validation.
B. Install the CloudTrail Processing Library.
C. Enable logging of Insights events in CloudTrail.
D. Enable custom logging from the on-premises resources.
E. Create an AWS Config rule to monitor whether CloudTrail is configured to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS).

Commented [LC439]: ANSWER

Commented [LC440]: ANSWER

Question #494

A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day, the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams.
What should a solutions architect do to resolve this issue?

A. Update the Kinesis Data Streams default settings by modifying the data retention period.
B. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

Commented [LC441]: A sufficient data retention period allows more time for your Kinesis stream data consumers to recover. The default retention period for an AWS Kinesis stream is 24 hours. To ensure that your consumers are able to read stream data before it expires if any problems occur, you can extend your data retention period up to 168 hours (7 days).

Question #495

A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event.
A solutions architect needs to design a solution that stores customer data that is created during database upgrades.
Which solution will meet these requirements?

A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.
B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.
C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.
D. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Commented [LC442]: ANSWER

Question #496

A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL.
What should a solutions architect do to meet these requirements?

A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.
C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Commented [LC443]: ANSWER

Question #497

A company has primary and secondary data centers that are 500 miles (804.7 km) apart and interconnected with high-speed fiber-optic cable. The company needs a highly available and secure network connection between its data centers and a VPC on AWS for a mission-critical workload. A solutions architect must choose a connection solution that provides maximum resiliency.
Which solution meets these requirements?

A. Two AWS Direct Connect connections from the primary data center terminating at two Direct Connect locations on two separate devices
B. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on the same device
C. Two AWS Direct Connect connections from each of the primary and secondary data centers terminating at two Direct Connect locations on two separate devices
D. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on two separate devices

Commented [LC444]: Since it's asking for Maximum resiliency, C is the answer

Question #498

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.
Which solution meets these requirements?

A. Enable a Multi-AZ deployment for the DB instance.
B. Enable auto scaling for the DB instance in one Availability Zone.
C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Commented [LC445]: Recovery point objective means that if one AZ doesn't respond, there's another backing up the situation.

Question #499

A company is hosting its website by using Amazon EC2 instances behind an Elastic Load Balancer across multiple Availability Zones. The instances run in an EC2 Auto Scaling group. The website uses Amazon Elastic Block Store (Amazon EBS) volumes to store product manuals for users to download. The company updates the product content often, so new instances launched by the Auto Scaling group often have old data. It can take up to 30 minutes for the new instances to receive all the updates. The updates also require the EBS volumes to be resized during business hours. The company wants to ensure that the product manuals are always up to date on all instances and that the architecture adjusts quickly to increased user demand. A solutions architect needs to meet these requirements without causing the company to update its application code or adjust its website. What should the solutions architect do to accomplish this goal?

A. Store the product manuals in an EBS volume. Mount that volume to the EC2 instances.
B. Store the product manuals in an Amazon S3 bucket. Redirect the downloads to this bucket.
C. Store the product manuals in an Amazon Elastic File System (Amazon EFS) volume. Mount that volume to the EC2 instances.
D. Store the product manuals in an Amazon S3 Standard-Infrequent Access (S3 Standard-IA) bucket. Redirect the downloads to this bucket.

Commented [LC446]: ANSWER

Questions from 501-505

Question #501

A company is building its web application by using containers on AWS. The company requires three instances of the web application to run at all times. The application must be highly available and must be able to scale to meet increases in demand.
Which solution meets these requirements?

A. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks.
B. Use the Amazon EC2 launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
C. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in three different Availability Zones. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks.
D. Use the Amazon EC2 launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance. Place one task on the remaining container instance.

Commented [LC447]: Fargate automatically scales to 3 AZ.

Ref. https://aws.amazon.com/it/blogs/containers/amazon-ecs-availability-best-practices/

Question #502

An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.
Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Commented [LC448]: ANSWER

Question #503

A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.
What should the solutions architect do to meet these requirements?

A. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.
B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
C. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Commented [LC449]: ANSWER

Question #504

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.
A solutions architect must design a solution to protect the application from this type of attack.
Which solution meets these requirements with the LEAST operational overhead?

A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Commented [LC450]: ANSWER

Question #505

A company is running an application on AWS to process weather sensor data that is stored in an Amazon S3 bucket. Three batch jobs run hourly to process the data in the S3 bucket for different purposes. The company wants to reduce the overall processing time by running the three applications in parallel using an event-based approach.
What should a solutions architect do to meet these requirements?

A. Enable S3 Event Notifications for new objects to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Subscribe all applications to the queue for processing.
B. Enable S3 Event Notifications for new objects to an Amazon Simple Queue Service (Amazon SQS) standard queue. Create an additional SQS queue for all applications, and subscribe all applications to the initial queue for processing.
C. Enable S3 Event Notifications for new objects to separate Amazon Simple Queue Service (Amazon SQS) FIFO queues. Create an additional SQS queue for each application, and subscribe each queue to the initial topic for processing.
D. Enable S3 Event Notifications for new objects to an Amazon Simple Notification Service (Amazon SNS) topic. Create an Amazon Simple Queue Service (Amazon SQS) queue for each application, and subscribe each queue to the topic for processing.

Commented [LC451]: Careful to the text: it's "for different purposes" so a SNS is necessary with 3 SQS standard queues.

Set of Questions #2

Questions 0-99

Question #0

A Solutions Architect is designing an application that will encrypt all data in an Amazon Redshift cluster. Which action will encrypt the data at rest?

A. Place the Redshift cluster in a private subnet.
B. Use the AWS KMS Default Customer master key.
C. Encrypt the Amazon EBS volumes.
D. Encrypt the data using SSL/TLS.

Commented [LC452]: ANSWER

Question #1

A website experiences unpredictable traffic. During peak traffic times, the database is unable to keep up with the write request. Which AWS service will help decouple the web application from the database?

A. Amazon SQS.
B. Amazon EFS.
C. Amazon S3.
D. AWS Lambda.

Commented [LC453]: ANSWER

Question #2

A legacy application needs to interact with local storage using iSCSI. A team needs to design a reliable storage solution to provision all new storage on AWS. Which storage solution meets the legacy application requirements?

A. AWS Snowball storage for the legacy application until the application can be re-architected.
B. AWS Storage Gateway in cached mode for the legacy application storage to write data to Amazon S3.
C. AWS Storage Gateway in stored mode for the legacy application storage to write data to Amazon S3.
D. An Amazon S3 volume mounted on the legacy application server locally using the File Gateway service.

Commented [LC454]: C is correct because Data is stored mainly in the legacy application but it's backed up on AWS.

Ref: https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-KM9E6jzVTQmseCrY7wb/gateway-stored-volumes-vs-gateway-cached-volumes

Question #3

A Solutions Architect is designing an architecture for a mobile gaming application. The application is expected to be very popular. The Architect needs to prevent the Amazon RDS MySQL database from becoming a bottleneck due to frequently accessed queries. Which service or feature should the Architect add to prevent a bottleneck?

A. Multi-AZ feature on the RDS MySQL Database.
B. ELB Classic Load Balancer in front of the web application tier.
C. Amazon SQS in front of RDS MySQL Database.
D. Amazon ElastiCache in front of the RDS MySQL Database.

Commented [LC455]: Frequently accessed query suggests the usage of a cache system, hence D.

Question #4

A company is launching an application that it expects to be very popular. The company needs a database that can scale with the rest of the application. The schema will change frequently. The application cannot afford any downtime for database changes. Which AWS service allows the company to achieve these objectives?

A. Amazon Redshift.
B. Amazon DynamoDB.
C. Amazon RDS MySQL.
D. Amazon Aurora.

Commented [LC456]: The schema will change frequently suggests a no-relational DB, like Dynamo

Question #5

A Solution Architect is designing a disaster recovery solution for a 5 TB Amazon Redshift cluster. The recovery site must be at least 500 miles (805 kilometers) from the live site. How should the Architect meet these requirements?

A. Use AWS CloudFormation to deploy the cluster in a second region.
B. Take a snapshot of the cluster and copy it to another Availability Zone.
C. Modify the Redshift cluster to span two regions.
D. Enable cross-region snapshots to a different region.

Commented [LC457]: ANSWER

Question #6

A customer has written an application that uses Amazon S3 exclusively as a data store. The application works well until the customer increases the rate at which the application is updating information. The customer now reports that outdated data occasionally appears when the application accesses objects in Amazon S3. What could be the problem, given that the application logic is otherwise correct?

A. The application is reading parts of objects from Amazon S3 using a range header.
B. The application is reading objects from Amazon S3 using parallel object requests.
C. The application is updating records by writing new objects with unique keys.
D. The application is updating records by overwriting existing objects with the same keys.

Commented [LC458]: Tricky question, see ref.

Ref. https://docs.aws.amazon.com/whitepapers/latest/s3-optimizing-performance-best-practices/use-byte-range-fetches.html

Question #7

A Solutions Architect is designing a new social media application. The application must provide a secure method for uploading profile photos. Each user should be able to upload a profile photo into a shared storage location for one week after their profile is created. Which approach will meet all of these requirements?

A. Use Amazon Kinesis with AWS CloudTrail for auditing the specific times when profile photos are uploaded.
B. Use Amazon EBS volumes with IAM policies restricting user access to specific time periods.
C. Use Amazon S3 with the default private access policy and generate pre-signed URLs each time a new site profile is created.
D. Use Amazon CloudFront with AWS CloudTrail for auditing the specific times when profile photos are uploaded.

Commented [LC459]: Classic pre-signed URL use case.

Question #8

An application requires block storage for file updates. The data is 500 GB and must continuously sustain 100 MiB/s of aggregate read/write operations. Which storage option is appropriate for this application?

A. Amazon S3.
B. Amazon EFS.
C. Amazon EBS.
D. Amazon Glacier.

Commented [LC460]: ANSWER

Question #9

A mobile application serves scientific articles from individual files in an Amazon S3 bucket. Articles older than 30 days are rarely read. Articles older than 60 days no longer need to be available through the application, but the application owner would like to keep them for historical purposes. Which cost - effective solution BEST meets these requirements?

A. Create a Lambda function to move files older than 30 days to Amazon EBS and move files older than 60 days to Amazon Glacier.
B. Create a Lambda function to move files older than 30 days to Amazon Glacier and move files older than 60 days to Amazon EBS.
C. Create lifecycle rules to move files older than 30 days to Amazon S3 Standard Infrequent Access and move files older than 60 days to Amazon Glacier.
D. Create lifecycle rules to move files older than 30 days to Amazon Glacier and move files older than 60 days to Amazon S3 Standard.

Commented [LC461]: ANSWER

Question #10

An organization is currently hosting a large amount of frequently accessed data consisting of key-value pairs and semi-structured documents in their data-center. They are planning to move this data to AWS. Which of one of the following services MOST effectively meets their needs?

A. Amazon Redshift.
B. Amazon RDS.
C. Amazon DynamoDB.
D. Amazon Aurora.

Commented [LC462]: ANSWER

Question #11

A Lambda function must execute a query against an Amazon RDS database in a private subnet. Which steps are required to allow the Lambda function to access the Amazon RDS database? (Select two.)

A. Create a VPC Endpoint for Amazon RDS.
B. Create the Lambda function within the Amazon RDS VPC.
C. Change the ingress rules of Lambda security group, allowing the Amazon RDS security group.
D. Change the ingress rules of the Amazon RDS security group, allowing the Lambda security group.
E. Add an Internet Gateway (IGW) to the VPC, route the private subnet to the IGW.

Commented [LC463]: ANSWER

Commented [LC464]: ANSWER

Question #12

A Solutions Architect needs to build a resilient data warehouse using Amazon Redshift. The Architect needs to rebuild the Redshift cluster in another region. Which approach can the Architect take to address this requirement?

A. Modify the Redshift cluster and Configure cross-region snapshots to the other region.

Commented [LC465]: ANSWER

B. Modify the Redshift cluster to take snapshots of the Amazon EBS volumes each day, sharing those snapshots with the other region.
C. Modify the Redshift cluster and Configure the backup and specify the Amazon S3 bucket in the other region.
D. Modify the Redshift cluster to use AWS Snowball in export mode with data delivered to the other region.

Question #13

A popular e-commerce application runs on AWS. The application encounters performance issues. The database is unable to handle the amount of queries and load during peak times. The database is running on the RDS Aurora engine on the largest instance size available. What should an administrator do to improve performance?

A. Convert the database to Amazon Redshift.
B. Create a CloudFront distribution.
C. Convert the database to use EBS Provisioned IOPS.
D. Create one or more read replicas.

Commented [LC466]: ANSWER

Question #14

A Solutions Architect is designing the architecture for a new three-tier web-based e-commerce site that must be available 24/7. Requests are expected to range from 100 to 10.000 each minute. Usage can vary depending on time of day, holidays, and promotions. The design should be able to handle these volumes, with the ability to handle higher volumes if necessary. How should the Architect design the architecture to ensure the web tier is cost-optimized and can handle the expected traffic? (Select two.)

A. Launch Amazon EC2 instances in an Auto Scaling group behind an ELB.

Commented [LC467]: ANSWER

B. Store all static files in a multi-AZ Amazon Aurora database.
C. Create an CloudFront distribution pointing to static content in Amazon S3.

Commented [LC468]: ANSWER

D. Use Amazon Route 53 to route traffic to the correct region.
E. Use Amazon S3 multi-part uploads to improve upload times.

Question #15

A Solution Architect is designing a three-tier web application. The Architect wants to restrict access to the database tier to accept traffic from the application servers only. However, these application servers are in an Auto Scaling group and may vary in quantity. How should the Architect Configure the database servers to meet the requirements?

A. Configure the database security group to allow database traffic from the application server IP addresses.
B. Configure the database security group to allow database traffic from the application server security group.

Commented [LC469]: ANSWER

C. Configure the database subnet network ACL to deny all inbound non-database traffic from the application-tier subnet.
D. Configure the database subnet network ACL to allow inbound database traffic from the application-tier subnet.

Question #16

An Internet-facing multi-tier web application must be highly available. An ELB Classic Load Balancer is deployed in front of the web tier. Amazon EC2 instances at the web application tier are deployed evenly across two Availability Zones. The database is deployed using RDS Multi-AZ. A NAT instance is launched for Amazon EC2 instances and database resources to access the Internet. These instances are not assigned with public IP addresses. Which component poses a potential single point of failure in this architecture?

A. Amazon EC2.
B. NAT instance.

Commented [LC470]: ANSWER

C. ELB Classic Load Balancer.
D. Amazon RDS.

Question #17

A call center application consists of a three - tier application using Auto Scaling groups to automatically scale resources as needed. Users report that every morning at 9:00 AM the system becomes very slow for about 15 minutes. A Solution Architect determines that a large percentage of the call center staff starts work at 9:00 AM, so Auto Scaling does not have enough time to scale out to meet demand. How can the Architect solve the problem?

A. Change the Auto Scaling group 's scale out event to scale based on network utilization.
B. Create an Auto Scaling scheduled action to scale out the necessary resources at 8:30 AM every morning.
C. Use Reserved Instances to ensure the system has reserved the right amount of capacity for the scale-up events.
D. Permanently keep a steady state of instances that is needed at 9:00 AM to guarantee available resources, but leverage Spot Instances.

Commented [LC471]: ANSWER

Question #18

An e-commerce application is hosted in AWS. The last time a new product was launched, the application experienced a performance issue due to an enormous spike in traffic. Management decided that capacity must be doubled the week after the product is launched. Which is the MOST efficient way for management to ensure that capacity requirements are met?

A. Add a Step Scaling policy.
B. Add a Dynamic Scaling policy.
C. Add a Scheduled Scaling action.
D. Add Amazon EC2 Spot Instances.

Commented [LC472]: This is another tricky question. The trick is in “after the product is launched”. Since we do not know when the product is going to be launched, we can’t use a “scheduled scaling action” policy. Hence, B.

Question #19

A customer owns a simple API for their website that receives about 1,000 requests each day and has an average response time of 50ms. It is currently hosted on one c4.large instance. Which changes to the architecture will provide high availability at the LOWEST cost?

A. Create an Auto Scaling group with a minimum of one instance and a maximum of two instances, then use an Application Load Balancer to balance the traffic.
B. Recreate the API using Amazon API Gateway and use AWS Lambda as the service backend.
C. Create an Auto Scaling group with a maximum of two instances, then use an Application Load Balancer to balance the traffic.
D. Recreate the API using Amazon API Gateway and integrate the new API with the existing backend service.

Commented [LC473]: ANSWER

Question #20

A Solution Architect is designing an application that uses Amazon EBS volumes. The volumes must be backed up to a different region. How should the Architect meet this requirement?

A. Create EBS snapshots directly from one region to another.
B. Move the data to an Amazon S3 bucket and enable cross-region replication.
C. Create EBS snapshots and then copy them to the desired region.
D. Use a script to copy data from the current Amazon EBS volume to the destination Amazon EBS volume.

Commented [LC474]: ANSWER

Question #21

A company is using an Amazon S3 bucket located in us-west-2 to serve videos to their customers. Their customers are located all around the world and the videos are requested a lot during peak hours. Customers in Europe complain about experiencing slow downloaded speeds, and during peak hours, customers in all locations report experiencing HTTP 500 errors. What can a Solutions Architect do to address these issues?

A. Place an elastic load balancer in front of the Amazon S3 bucket to distribute the load during peak hours.
B. Cache the web content with Amazon CloudFront and use all Edge locations for content delivery.
C. Replicate the bucket in eu-west-1 and use an Amazon Route 53 failover routing policy to determine which bucket it should serve the request to.
D. Use an Amazon Route 53 weighted routing policy for the CloudFront domain name to distribute the GET request between CloudFront and the Amazon S3 bucket directly.

Commented [LC475]: ANSWER

Question #22

A Solutions Architect is designing a solution that includes a managed VPN connection. To monitor whether the VPN connection is up or down, the Architect should use:

A. An external service to ping the VPN endpoint from outside the VPC.
B. AWS CloudTrail to monitor the endpoint.
C. The CloudWatch TunnelState Metric.
D. An AWS Lambda function that parses the VPN connection logs.

Commented [LC476]: ANSWER

Question #23

A social networking portal experiences latency and throughput issues due to an increased number of users. Application servers use very large datasets from an Amazon RDS database, which creates a performance bottleneck on the database. Which AWS service should be used to improve performance?

A. Auto Scaling.
B. Amazon SQS.
C. Amazon ElastiCache.
D. ELB Application Load Balancer.

Commented [LC477]: ElastiCache creates a caching layer and fills the purpose.

Question #24

A Solutions Architect is designing network architecture for an application that has compliance requirements. The application will be hosted on Amazon EC2 instances in a private subnet and will be using Amazon S3 for storing data. The compliance requirements mandate that the data cannot traverse the public Internet. What is the MOST secure way to satisfy this requirement?

A. Use a NAT Instance.
B. Use a NAT Gateway.
C. Use a VPC endpoint.
D. Use a Virtual Private Gateway.

Commented [LC478]: ANSWER

Question #25

Developers are creating a new online transaction processing (OLTP) application for a small database that is very read-write intensive. A single table in the database is updated continuously throughout the day, and the developers want to ensure that the database performance is consistent. Which Amazon EBS storage option will achieve the MOST consistent performance to help maintain application performance?

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

Commented [LC479]: ANSWER

Question #26

A Solutions Architect is designing a log-processing solution that requires storage that supports up to 500 MB/s throughput. The data is sequentially accessed by an Amazon EC2 instance. Which Amazon storage type satisfies these requirements?

A. EBS Provisioned IOPS SSD (io1).
B. EBS General Purpose SSD (gp2).
C. EBS Throughput Optimized HDD (st1).
D. EBS Cold HDD (sc1).

Commented [LC480]: C is correct, see ref for the chart.

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

Question #27

A company's development team plans to create an Amazon S3 bucket that contains millions of images. The team wants to maximize the read performance of Amazon S3. Which naming scheme should the company use?

A. Add a date as the prefix.
B. Add a sequential id as the suffix.
C. Add a hexadecimal hash as the suffix.
D. Add a hexadecimal hash as the prefix.

Commented [LC481]: B is correct.

Ref. https://aws.amazon.com/premiumsupport/knowledge-center/s3-object-key-naming-pattern/

Question #28

A Solutions Architect needs to design a solution that will enable a security team to detect, review, and perform root cause analysis of security incidents that occur in a cloud environment. The Architect must provide a centralized view of all API events for current and future AWS regions. How should the Architect accomplish this task?

A. Enable AWS CloudTrail logging in each individual region. Repeat this for all future regions.
B. Enable Amazon CloudWatch logs for all AWS services across all regions and aggregate them in a single Amazon S3 bucket.
C. Enable AWS Trusted Advisor security checks and report all security incidents for all regions.
D. Enable AWS CloudTrail by creating a new trail and apply the trail to all regions.

Commented [LC482]: Answer is B.

Trusted Advisor is not an enabler.

https://aws.amazon.com/it/premiumsupport/technology/trusted-advisor/

Question #29

A company has a legacy application using a proprietary file system and plans to migrate the application to AWS. Which storage service should the company use?

A. Amazon DynamoDB.
B. Amazon S3.
C. Amazon EBS.
D. Amazon EFS.

Commented [LC483]: the answer is: EFS

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

This is not specified but in theory you could access EFS file systems from on-premises, you must have an AWS Direct Connect or AWS VPN connection between your on-premises datacenter and your Amazon VPC.

You mount an EFS file system on your on-premises Linux server using the standard Linux mount command for mounting a file system via the NFSv4.1 protocol.

Question #30

A company plans to use AWS for all new batch processing workloads. The company's developers use Docker containers for the new batch processing. The system design must accommodate critical and non-critical batch processing workloads 24/7. How should a Solutions Architect design this architecture in a cost-efficient manner?

A. Purchase Reserved Instances to run all containers. Use Auto Scaling groups to schedule jobs.
B. Host a container management service on Spot Instances. Use Reserved Instances to run Docker containers.
C. Use Amazon ECS orchestration and Auto Scaling groups: one with Reserve Instances, one with Spot Instances.
D. Use Amazon ECS to manage container orchestration. Purchase Reserved Instances to run all batch workloads at the same time.

Commented [LC484]: ANSWER

Question #31

A company is evaluating Amazon S3 as a data storage solution for their daily analyst reports. The company has implemented stringent requirements concerning the security of the data at rest. specifically, the CISO asked for the use of envelope encryption with separate permissions for the use of an envelope key, automated rotation of the encryption keys, and visibility into when an encryption key was used and by whom. Which steps should a Solutions Architect take to satisfy the security requirements requested by the CISO?

A. Create an Amazon S3 bucket to store the reports and use Server-Side Encryption with Customer-Provided Keys (SSE-C).
B. Create an Amazon S3 bucket to store the reports and use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).
C. Create an Amazon S3 bucket to store the reports and use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).
D. Create an Amazon S3 bucket to store the reports and use Amazon S3 versioning with Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).

Commented [LC485]: Ref.
https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

https://acloud.guru/forums/aws-csa-2019/discussion/-Lynz2jue99SX6UFdlgg/what

Question #32

A customer has a production application that frequently overwrites and deletes data, the application requires the most up-to-date version of the data every time it is requested. Which storage should a Solutions Architect recommend to bet accommodate this use case?

A. Amazon S3.
B. Amazon RDS.
C. Amazon RedShift.
D. AWS Storage Gateway.

Commented [LC486]: Amazon S3 is the only Storage Service among the answers.

Question #33

A Solutions Architect is designing a photo application on AWS. Every time a user uploads a photo to Amazon S3, the Architect must insert a new item to a DynamoDB table. Which AWS-managed service is the BEST to insert the item?

A. Lambda@Edge.
B. AWS Lambda.
C. Amazon API Gateway.
D. Amazon EC2 instances.

Commented [LC487]: ANSWER

Question #34

An application relies on messages being sent and received in order. The volume will never exceed more than 300 transactions each second. Which service should be used?

A. Amazon SQS.
B. Amazon SNS.
C. Amazon ECS.
D. AWS STS.

Commented [LC488]: ANSWER

Question #35

A Solutions Architect is designing an application on AWS that uses persistent block storage. Data must be encrypted at rest. Which solution meets the requirement?

A. Enable SSL on Amazon EC2 instances.
B. Encrypt Amazon EBS volumes on Amazon EC2 instances.
C. Enable server-side encryption on Amazon S3.
D. Encrypt Amazon EC2 Instance Storage.

Commented [LC489]: ANSWER

Question #36

A company is launching a static website using the zone apex (mycompany.com). The company wants to use Amazon Route 53 for DNS. Which steps should the company perform to implement a scalable and cost-effective solution? (Choose two.)

A. Host the website on an Amazon EC2 instance with ELB and Auto Scaling, and map a Route 53 alias record to the ELB endpoint.
B. Host the website using AWS Elastic Beanstalk, and map a Route 53 alias record to the Beanstalk stack.
C. Host the website on an Amazon EC2 instance, and map a Route 53 alias record to the public IP address of the Amazon EC2 instance.
D. Serve the website from an Amazon S3 bucket, and map a Route 53 alias record to the website endpoint.
E. Create a Route 53 hosted zone, and set the NS records of the domain to use Route 53 name servers.

Commented [LC490]: ANSWER

Commented [LC491]: ANSWER

Question #37

A manufacturing company captures data from machines running at customer sites. Currently, thousands of machines send data every 5 minutes, and this is expected to grow to hundreds of thousands of machines in the near future. The data is logged with the intent to be analysed in the future as needed. What is the SIMPLEST method to store this streaming data at scale?

A. Create an Amazon Kinesis Firehouse delivery stream to store the data in Amazon S3.
B. Create an Auto Scaling group of Amazon EC2 servers behind ELBs to write the data into Amazon RDS.
C. Create an Amazon SQS queue, and have the machines write to the queue.
D. Create an Amazon EC2 server farm behind an ELB to store the data in Amazon EBS Cold HDD volumes.

Commented [LC492]: ANSWER

Question #38

A bank is writing new software that is heavily dependent upon the database transactions for write consistency. The application will also occasionally generate reports on data in the database, and will do joins across multiple tables. The database must automatically scale as the amount of data grows. Which AWS service should be used to run the database?

A. Amazon S3.
B. Amazon Aurora.
C. Amazon DynamoDB.
D. Amazon Redshift.

Commented [LC493]: ANSWER

Question #39

A Solutions Architect is designing a new application that needs to access data in a different AWS account located within the same region. The data must not be accessed over the Internet. Which solution will meet these requirements with the LOWEST cost?

A. Add rules to the security groups in each account.
B. Establish a VPC Peering connection between accounts.
C. Configure Direct Connect in each account.
D. Add a NAT Gateway to the data account.

Commented [LC494]: ANSWER

Question #40

A Solutions Architect is designing a mobile application that will capture receipt images to track expenses. The Architect wants to store the images on Amazon S3. However, uploading images through the web server will create too much traffic. What is the MOST efficient method to store images from a mobile application on Amazon S3?

A. Upload directly to S3 using a pre-signed URL.
B. Upload to a second bucket, and have Lambda event copy the image to the primary bucket.
C. Upload to a separate Auto Scaling group of servers behind an ELB Classic Load Balancer, and have them write to the Amazon S3 bucket.
D. Expand the web server fleet with Spot Instances to provide the resources to handle the images.

Commented [LC495]: ANSWER

Question #41

A company requires that the source, destination, and protocol of all IP packets be recorded when traversing a private subnet. What is the MOST secure and reliable method of accomplishing this goal.

A. Create VPC flow logs on the subnet.
B. Enable source destination check on private Amazon EC2 instances.
C. Enable AWS CloudTrail logging and specify an Amazon S3 bucket for storing log files.
D. Create an Amazon CloudWatch log to capture packet information.

Commented [LC496]: ANSWER

Question #42

A Solutions Architect has a multi-layer application running in Amazon VPC. The application has an ELB Classic Load Balancer as the front end in a public subnet, and an Amazon EC2-based reverse proxy that performs content-based routing to two backend Amazon EC2 instances hosted in a private subnet. The Architect sees tremendous traffic growth and is concerned that the reverse proxy and current backend set up will be insufficient. Which actions should the Architect take to achieve a cost-effective solution that ensures the application automatically scales to meet traffic demand? (Select two.)

A. Replace the Amazon EC2 reverse proxy with an ELB internal Classic Load Balancer.
B. Add Auto Scaling to the Amazon EC2 backend fleet.
C. Add Auto Scaling to the Amazon EC2 reverse proxy layer.
D. Use t2 burstable instance types for the backend fleet.
E. Replace both the frontend and reverse proxy layers with an ELB Application Load Balancer.

Commented [LC497]: ANSWER

Commented [LC498]: ANSWER

Question #43

A company is launching a marketing campaign on their website tomorrow and expects a significant increase in traffic. The website is designed as a multi-tiered web architecture, and the increase in traffic could potentially overwhelm the current design. What should a Solutions Architect do to minimize the effects from a potential failure in one or more of the tiers?

A. Migrate the database to Amazon RDS.
B. Set up DNS failover to a statistic website.
C. Use Auto Scaling to keep up with the demand.
D. Use both a SQL and a NoSQL database in the design.

Commented [LC499]: ANSWER

Question #44

A web application experiences high compute costs due to serving a high amount of static web content. How should the web server architecture be designed to be the MOST cost-efficient?

A. Create an Auto Scaling group to scale out based on average CPU usage.
B. Create an Amazon CloudFront distribution to pull static content from an Amazon S3 bucket.
C. Leverage Reserved Instances to add additional capacity at a significantly lower price.
D. Create a multi-region deployment using an Amazon Route 53 geolocation routing policy.

Commented [LC500]: ANSWER

Question #45

A Solutions Architect plans to migrate NAT instances to NAT gateway. The Architect has NAT instances with scripts to manage high availability. What is the MOST efficient method to achieve similar high availability with NAT gateway?

A. Remove source/destination check on NAT instances.
B. Launch a NAT gateway in each Availability Zone.
C. Use a mix of NAT instances and NAT gateway.
D. Add an ELB Application Load Balancer in front of NAT gateway.

Commented [LC501]: ANSWER

Question #46

A Solutions Architect is designing a solution to store a large quantity of event data in Amazon S3. The Architect anticipates that the workload will consistently exceed 100 requests each second. What should the Architect do in Amazon S3 to optimize performance?

A. Randomize a key name prefix.
B. Store the event data in separate buckets.
C. Randomize the key name suffix.
D. Use Amazon S3 Transfer Acceleration.

Commented [LC502]: Technically the answer would be A but at the current state of S3 there's no need anymore of doing that.

See.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/optimizing-performance.html

S3 Transfer Acceleration is wrong because it's used to reduce transfer of geographically long distant locations

Question #47

A user is testing a new service that receives location updates from 3,600 rental cars every hour. Which service will collect data and automatically scale to accommodate production workload?

A. Amazon EC2.
B. Amazon Kinesis Firehose.
C. Amazon EBS.
D. Amazon API Gateway.

Commented [LC503]: ANSWER

Question #48

A Solutions Architect is designing a web application. The web and application tiers need to access the Internet, but they cannot be accessed from the Internet. Which of the following steps is required?

A. Attach an Elastic IP address to each Amazon EC2 instance and add a route from the private subnet to the public subnet.
B. Launch a NAT gateway in the public subnet and add a route to it from the private subnet.
C. Launch Amazon EC2 instances in the public subnet and change the security group to allow outbound traffic on port 80.
D. Launch a NAT gateway in the private subnet and deploy a NAT instance in the private subnet.

Commented [LC504]: ANSWER

Question #49

An application stack includes an Elastic Load Balancer in a public subnet, a fleet of Amazon EC2 instances in an Auto Scaling group, and an Amazon RDS MySQL cluster. Users connect to the application from the Internet. The application servers and database must be secure. How should a Solutions Architect perform this task?

A. Create a private subnet for the Amazon EC2 instances and a public subnet for the Amazon RDS cluster.
B. Create a private subnet for the Amazon EC2 instances and a private subnet for the Amazon RDS cluster.
C. Create a public subnet for the Amazon EC2 instances and a private subnet for the Amazon RDS cluster.
D. Create a public subnet for the Amazon EC2 instances and a public subnet for the Amazon RDS cluster.

Commented [LC505]: ANSWER

Question #50

A Solutions Architect is designing a solution for a media company that will stream large amounts of data from an Amazon EC2 instance. The data streams are typically large and sequential, and must be able to support up to 500 MB/s. Which storage type will meet the performance requirements of this application?

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

Commented [LC506]: ANSWER

Question #51

A legacy application running in premises requires a Solutions Architect to be able to open a firewall to allow access to several Amazon S3 buckets. The Architect has a VPN connection to AWS in place. How should the Architect meet this requirement?

A. Create an IAM role that allows access from the corporate network to Amazon S3.
B. Configure a proxy on Amazon EC2 and use an Amazon S3 VPC endpoint.
C. Use Amazon API Gateway to do IP whitelisting.
D. Configure IP whitelisting on the customer's gateway.

Commented [LC507]: ANSWER

Question #52

A Solutions Architect is designing a database solution that must support a high rate of random disk reads and writes. It must provide consistent performance, and requires long - term persistence. Which storage solution BEST meets these requirements?

A. An Amazon EBS Provisioned IOPS volume.
B. An Amazon EBS General Purpose volume.
C. An Amazon EBS Magnetic volume.
D. An Amazon EC2 Instance Store.

Commented [LC508]: Ref. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Question #53

A Solutions Architect is designing solution with AWS Lambda where different environments require different database passwords. What should the Architect do to accomplish this in a secure and scalable way?

A. Create a Lambda function for each individual environment.
B. Use Amazon DynamoDB to store environmental variables.
C. Use encrypted AWS Lambda environmental variables.
D. Implement a dedicated Lambda function for distributing variables.

Commented [LC509]: https://docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html

Question #54

A news organization plans to migrate their 20 TB video archive to AWS. The files are rarely accessed, but when they are, a request is made in advance and a 3 to 5 - hour retrieval time frame is acceptable. However, when there is a breaking news story, the editors require access to archived footage within minutes. Which storage solution meets the needs of this organization while providing the LOWEST cost of storage?

A. Store the archive in Amazon S3 Reduced Redundancy Storage.
B. Store the archive in Amazon Glacier and use standard retrieval for all content.
C. Store the archive in Amazon Glacier and pay the additional charge for expedited retrieval when needed.
D. Store the archive in Amazon S3 with a lifecycle policy to move this to S3 Infrequent Access after 30 days.

Commented [LC510]: ANSWER

Question #55

A Solutions Architect is building a multi-tier website. The web servers will be in a public subnet, and the database servers will be in a private subnet. Only the web servers can be accessed from the Internet. The database servers must have Internet access for software updates. Which solution meets the requirements?

A. Assign Elastic IP addresses to the database instances.
B. Allow Internet traffic on the private subnet through the network ACL.
C. Use a NAT Gateway.
D. Use an egress-only Internet Gateway.

Commented [LC511]: ANSWER

Question #56

A Solutions Architect is designing a Lambda function that calls an API to list all running Amazon RDS instances. How should the request be authorized?

A. Create an IAM access and secret key, and store it in the Lambda function.
B. Create an IAM role to the Lambda function with permissions to list all Amazon RDS instances.
C. Create an IAM role to Amazon RDS with permissions to list all Amazon RDS instances.
D. Create an IAM access and secret key, and store it in an encrypted RDS database.

Commented [LC512]: ANSWER

Question #57

A Solutions Architect is building an application on AWS that will require 20,000 IOPS on a particular volume to support a media event. Once the event ends, the IOPS need is no longer required. The marketing team asks the Architect to build the platform to optimize storage without incurring downtime. How should the Architect design the platform to meet these requirements?

A. Change the Amazon EC2 instant types.
B. Change the EBS volume type to Provisioned IOPS.
C. Stop the Amazon EC2 instance and provision IOPS for the EBS volume.
D. Enable an API Gateway to change the endpoints for the Amazon EC2 instances.

Commented [LC513]: ANSWER

Question #58

A Solutions Architect is building a new feature using a Lambda to create metadata when a user uploads a picture to Amazon S3. All metadata must be indexed. Which AWS service should the Architect use to store this metadata?

A. Amazon S3.
B. Amazon DynamoDB.
C. Amazon Kinesis.
D. Amazon EFC.

Commented [LC514]: ANSWER

Question #59

An interactive, dynamic website runs on Amazon EC2 instances in a single subnet behind an ELB Classic Load Balancer. Which design changes will make the site more highly available?

A. Move some Amazon EC2 instances to a subnet in a different way.
B. Move the website to Amazon S3.
C. Change the ELB to an Application Load Balancer.
D. Move some Amazon EC2 instances to a subnet in the same Availability Zone.

Commented [LC515]: Even though the "different way" is not specified, it's the only correct answer. B is wrong because S3 can't host dynamic websites. C is wrong because an ALB is not enough to ensure HA. D is wrong because it's not a HA solution.

Question #60

A Solutions Architect is designing a web application that is running on an Amazon EC2 instance. The application stores data in DynamoDB. The Architect needs to secure access to the DynamoDB table. What combination of steps does AWS recommend to achieve secure authorization? (Select two.)

A. Store an access key on the Amazon EC2 instance with rights to the Dynamo DB table.
B. Attach an IAM user to the Amazon EC2 instance.
C. Create an IAM role with permissions to write to the DynamoDB table.
D. Attach an IAM role to the Amazon EC2 instance.
E. Attach an IAM policy to the Amazon EC2 instance.

Commented [LC516]: ANSWER

Commented [LC517]: ANSWER

Question #61

A Solutions Architect is about to deploy an API on multiple EC2 instances in an Auto Scaling group behind an ELB. The support team has the following operational requirements:

1 They get an alert when the requests per second go over 50,000;

2 They get an alert when latency goes over 5 seconds;

3 They can validate how many times a day users call the API requesting highly-sensitive data;

Which combination of steps does the Architect need to take to satisfy these operational requirements? (Select two.)

A. Ensure that CloudTrail is enabled.
B. Create a custom CloudWatch metric to monitor the API for data access.
C. Configure CloudWatch alarms for any metrics the support team requires.
D. Ensure that detailed monitoring for the EC2 instances is enabled.
E. Create an application to export and save CloudWatch metrics for longer term trending analysis.

Commented [LC518]: ANSWER

Commented [LC519]: ANSWER

Question #62

A Solutions Architect is designing a highly-available website that is served by multiple web servers hosted outside of AWS. If an instance becomes unresponsive, the Architect needs to remove it from the rotation. What is the MOST efficient way to fulfil this requirement?

A. Use Amazon CloudWatch to monitor utilization.
B. Use Amazon API Gateway to monitor availability.
C. Use an Amazon Elastic Load Balancer.
D. Use Amazon Route 53 health checks.

Commented [LC520]: ANSWER

Question #63

A company hosts a popular web application. The web application connects to a database running in a private VPC subnet. The web servers must be accessible only to customers on an SSL connection. The RDS MySQL database server must be accessible only from the web servers. How should the Architect design a solution to meet the requirements without impacting running applications?

A. Create a network ACL on the web server's subnet, and allow HTTPS inbound and MySQL outbound. Place both database and web servers on the same subnet.
B. Open an HTTPS port on the security group for web servers and set the source to 0.0.0.0/0. Open the MySQL port on the database security group and attach it to the MySQL instance. Set the source to Web Server Security Group.
C. Create a network ACL on the web server's subnet, and allow HTTPS inbound, and specify the source as 0.0.0.0/0. Create a network ACL on a database subnet, allow MySQL port inbound for web servers, and deny all outbound traffic.
D. Open the MySQL port on the security group for web servers and set the source to 0.0.0.0/0. Open the HTTPS port on the database security group and attach it to the MySQL instance. Set the source to Web Server Security Group.

Commented [LC521]: ANSWER

Question #64

Which service should an organization use if it requires an easily managed and scalable platform to host its web application running on Nginx?

A. AWS Lambda.
B. Auto Scaling.
C. AWS Elastic Beanstalk.
D. Elastic Load Balancing.

Commented [LC522]: ANSWER

Question #65

An Administrator is hosting an application on a single Amazon EC2 instance, which users can access by the public hostname. The administrator is adding a second instance, but does not want users to have to decide between many public hostnames. Which AWS service will decouple the users from specific Amazon EC2 instances?

A. Amazon SQS.
B. Auto Scaling group.
C. Amazon EC2 security group.
D. Amazon ELB.

Commented [LC523]: ANSWER

Question #66

A Solutions Architect is designing a microservices based application using Amazon ECS. The application includes a WebSocket component, and the traffic needs to be distributed between microservices based on the URL. Which service should the Architect choose to distribute the workload?

A. ELB Classic Load Balancer.
B. Amazon Route 53 DNS.
C. ELB Application Load Balancer.
D. Amazon CloudFront.

Commented [LC524]: Path-based routing is possible with ALB: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-application-load-balancer-cli.html#path-based-routing-aws-cli

Question #67

A Solutions Architect is designing the storage layer for a production relational database. The database will run on Amazon EC2. The database is accessed by an application that performs intensive reads and writes, so the database requires the LOWEST random I/O latency. Which data storage method fulfils the above requirements?

A. Store data in a filesystem backed by Amazon Elastic File System (EFS).
B. Store data in Amazon S3 and use a third-party solution to expose Amazon S3 as a filesystem to the database server.
C. Store data in Amazon Dynamo DB and emulate relational database semantics.
D. Stripe data across multiple Amazon EBS volumes using RAID 0.

Commented [LC525]: ANSWER

Question #68

A Solutions Architect is designing a VPC. Instances in a private subnet must be able to establish IPv6 traffic to the Internet. The design must scale automatically and not incur any additional cost. This can be accomplished with:

A. an egress-only internet gateway.
B. a NAT gateway.
C. a custom NAT instance.
D. a VPC endpoint.

Commented [LC526]: ANSWER

Question #69

A web application stores all data in an Amazon RDS Aurora database instance. A Solutions Architect wants to provide access to the data for a detailed report for the Marketing team, but is concerned that the additional load on the database will affect the performance of the web application. How can the report be created without affecting the performance of the application?

A. Create a read replica of the database.
B. Provision a new RDS instance as a secondary master.
C. Configure the database to be in multiple regions.
D. Increase the number of provisioned storage IOPS.

Commented [LC527]: ANSWER

Question #70

A company has an application that stores sensitive data. The company is required by government regulations to store multiple copies of its data. What would be the MOST resilient and cost-effective option to meet this requirement?

A. Amazon EFS.
B. Amazon RDS.
C. AWS Storage Gateway.
D. Amazon S3.

Commented [LC528]: ANSWER

Question #71

A company is using AWS Key Management Service (AWS KMS) to secure their Amazon RDS databases. An auditor has recommended that the company log all use of their AWS KMS keys. What is the SIMPLEST solution?

A. Associate AWS KMS metrics with Amazon CloudWatch.
B. Use AWS CloudTrail to log AWS KMS key usage.
C. Deploy a monitoring agent on the RDS instances.
D. Poll AWS KMS periodically with a scheduled job.

Commented [LC529]: ANSWER

Question #72

A Solutions Architect is designing a stateful web application that will run for one year (24/7) and then be decommissioned. Load on this platform will be constant, using a number of r4.8xlarge instances. Key drivers for this system include high availability, but elasticity is not required. What is the MOST cost-effective way to purchase compute for this platform?

A. Scheduled Reserved Instances.
B. Convertible Reserved Instances.
C. Standard Reserved Instances.
D. Spot Instances.

Commented [LC530]: Standard Reserved Instances can be bought for a definite time interval like a year to have the best price.

Scheduled Reserved Instances (disbanded) were instances available for a specific time range (i.e. every wed between 10-13).

Question #73

A media company asked a Solutions Architect to design a highly available storage solution to serve as a centralized document store for their Amazon EC2 instances. The storage solution needs to be POSIX-compliant, scale dynamically, and be able to serve up to 100 concurrent EC2 instances. Which solution meets these requirements?

A. Create an Amazon S3 bucket and store all of the documents in this bucket.
B. Create an Amazon EBS volume and allow multiple users to mount that volume to their EC2 instance(s).
C. Use Amazon Glacier to store all of the documents.
D. Create an Amazon Elastic File System (Amazon EFS) to store and share the documents.

Commented [LC531]: ANSWER

Question #74

A Solution Architect has a two-tier application with a single Amazon EC2 instance web server and Amazon RDS MySQL Multi-AZ DB instances. The Architect is re-architecting the application for high availability by adding instances in a second Availability Zone. Which additional services will improve the availability of the application? (Choose two.)

A. Auto Scaling group.
B. AWS CloudTrail.
C. ELB Classic Load Balancer.
D. Amazon DynamoDB.
E. Amazon ElastiCache.

Commented [LC532]: ANSWER

Commented [LC533]: ANSWER

Question #75

A company is migrating its data center to AWS. As part of this migration, there is a three-tier web application that has strict data-at-rest encryption requirements. The customer deploys this application on Amazon EC2 using Amazon EBS, and now must provide encryption at-rest. How can this requirement be met without changing the application?

A. Use AWS Key Management Service and move the encrypted data to Amazon S3.
B. Use an application-specific encryption API with AWS server-side encryption.
C. Use encrypted EBS storage volumes with AWS-managed keys.
D. Use third-party tools to encrypt the EBS data volumes with Key Management Service Bring Your Own Keys.

Commented [LC534]: ANSWER

Question #76

A Solutions Architect is developing software on AWS that requires access to multiple AWS services, including an Amazon EC2 instance. This is a security sensitive application, and AWS credentials such as Access Key ID and Secret Access Key need to be protected and cannot be exposed anywhere in the system. What security measure would satisfy these requirements ?

A. Store the AWS Access Key ID / Secret Access Key combination in software comments.
B. Assign an IAM user to the Amazon EC2 instance.
C. Assign an IAM role to the Amazon EC2 instance.
D. Enable multi - factor authentication for the AWS root account.

Commented [LC535]: ANSWER

Question #77

An AWS workload in a VPC is running a legacy database on an Amazon EC2 instance. Data is stored on a 200GB Amazon EBS (gp2) volume. At peak load times, logs show excessive wait time. What solution should be implemented to improve database performance using persistent storage?

A. Migrate the data on the Amazon EBS volume to an SSD-backed volume.
B. Change the EC2 instance type to one with EC2 instance store volumes.
C. Migrate the data on the EBS volume to provisioned IOPS SSD (io1).
D. Change the EC2 instance type to one with burstable performance.

Commented [LC536]: ANSWER

Question #78

A company's website receives 50,000 requests each second, and the company wants to use multiple applications to analyse the navigation patterns of the users on their website so that the experience can be personalized. What can a Solutions Architect use to collect page clicks for the website and process them sequentially for each user?

A. Amazon Kinesis Stream.
B. Amazon SQS standard queue.
C. Amazon SQS FIFO queue.
D. AWS CloudTrail trail.

Commented [LC537]: ANSWER

Question #79

A company wants to migrate a highly transactional database to AWS. Requirements state that the database has more than 6 TB of data and will grow exponentially. Which solution should a Solutions Architect recommend?

A. Amazon Aurora.
B. Amazon Redshift.
C. Amazon DynamoDB.
D. Amazon RDS MySQL.

Commented [LC538]: ANSWER

Question #80

A company hosts a two-tier application that consists of a publicly accessible web server that communicates with a private database. Only HTTPS port 443 traffic to the web server must be allowed from the Internet. Which of the following options will achieve these requirements? (Choose two.)

A. Security group rule that allows inbound Internet traffic for port 443.
B. Security group rule that denies all inbound Internet traffic except port 443.
C. Network ACL rule that allows port 443 inbound and all ports outbound for Internet traffic.
D. Security group rule that allows Internet traffic for port 443 in both inbound and outbound.
E. Network ACL rule that allows port 443 for both inbound and outbound for all Internet traffic.

Commented [LC539]: ANSWER

Commented [LC540]: C over E because the question doesn't ask to restrict other outbound ports.

Question #81

A Solutions Architect is designing an Amazon VPC. Applications in the VPC must have private connectivity to Amazon DynamoDB in the same AWS Region. The design should route DynamoDB traffic through:

A. VPC peering connection.
B. NAT gateway.
C. VPC endpoint.
D. AWS Direct Connect.

Commented [LC541]: ANSWER

Question #82

A Solutions Architect is architecting a workload that requires a performant object-based storage system that must be shared with multiple Amazon EC2 instances. Which AWS service meets this requirement?

A. Amazon EFS.
B. Amazon S3.
C. Amazon EBS.
D. Amazon ElastiCache.

Commented [LC542]: EFS is NOT a object-based storage system, so answer must be S3

Question #83

A Solutions Architect is developing a solution for sharing files in an organization. The solution must allow multiple users to access the storage service at once from different virtual machines and scale automatically. It must also support file-level locking. Which storage service meets the requirements of this use case?

A. Amazon S3.
B. Amazon EFS.
C. Amazon EBS.
D. Cached Volumes.

Commented [LC543]: ANSWER

Question #84

A company runs a legacy application with a single-tier architecture on an Amazon EC2 instance. Disk I/O is low, with occasional small spikes during business hours. The company requires the instance to be stopped from 8 PM to 8 AM daily. Which storage option is MOST appropriate for this workload?

A. Amazon EC2 instance storage.
B. Amazon EBS General Purpose SSD (gp2) storage.
C. Amazon S3.
D. Amazon EBS Provision IOPS SSD (io1) storage.

Commented [LC544]: ANSWER

Question #85

As part of securing an API layer built on Amazon API gateway, a Solutions Architect has to authorize users who are currently authenticated by an existing identity provider. The users must be denied access for a period of one hour after three unsuccessful attempts. How can the Solutions Architect meet these requirements?

A. Use AWS IAM authorization and add least-privileged permissions to each respective IAM role.
B. Use an API Gateway custom authorizer to invoke an AWS Lambda function to validate each user's identity.
C. Use Amazon Cognito user pools to provide built-in user management.
D. Use Amazon Cognito user pools to integrate with external identity providers.

Commented [LC545]: ANSWER

Question #86

An organization runs an online media site, hosted on-premises. An employee posted a product review that contained videos and pictures. The review went viral and the organization needs to handle the resulting spike in website traffic. What action would provide an immediate solution?

A. Redesign the website to use Amazon API Gateway, and use AWS Lambda to deliver content.
B. Add server instances using Amazon EC2 and use Amazon Route 53 with a failover routing policy.
C. Serve the images and videos via an Amazon CloudFront distribution created using the news site as the origin.
D. Use Amazon ElasticCache for Redis for caching and reducing the load requests from the origin.

Commented [LC546]: ANSWER

Question #87

A client notices that their engineers often make mistakes when creating Amazon SQS queues for their backend system. Which action should a Solutions Architect recommend to improve this process?

A. Use the AWS CLI to create queues using AWS IAM Access Keys.
B. Write a script to create the Amazon SQS queue using AWS Lambda.
C. Use AWS Elastic Beanstalk to automatically create the Amazon SQS queues.
D. Use AWS CloudFormation Templates to manage the Amazon SQS queue creation.

Commented [LC547]: ANSWER

Question #88

A development team is building an application with frontend and backend application tiers. Each tier consists of Amazon EC2 instances behind an ELB Classic Load Balancer. The instances run in Auto Scaling groups across multiple Availability Zones. The network team has allocated the 10.0.0.0/24 address space for this application. Only the front-end load balancer should be exposed to the Internet. There are concerns about the limited size of the address space and the ability of each tier to scale. What should the VPC subnet design be in each Availability Zone?

A. One public subnet for the load balancer tier, one public subnet for the front-end tier, and one private subnet for the backend tier.
B. One shared public subnet for all tiers of the application.
C. One public subnet for the load balancer tier and one shared private subnet for the application tiers.
D. One shared private subnet for all tiers of the application.

Commented [LC548]: ANSWER

Question #89

A Solutions Architect must select the storage type for a big data application that requires very high sequential I/O. The data must persist if the instance is stopped. Which of the following storage types will provide the best at the LOWEST cost for the application?

A. An Amazon EC2 instance store local SSD volume.
B. An Amazon EBS provisioned IOPS SSD volume.
C. An Amazon EBS throughput optimized HDD volume.
D. An Amazon EBS general purpose SSD volume.

Commented [LC549]: Tricky and unsure about this. If the priority is COST then C should be our point. If performance is our priority then it's B.

Question #90

Two Auto Scaling applications, Application A and Application B, currently run within a shared set of subnets. A Solutions Architect wants to make sure that Application A can make requests to Application B, but Application B should be denied from making requests to Application A. Which is the SIMPLEST solution to achieve this policy?

A. Using security groups that reference the security groups of the other application.
B. Using security groups that reference the application server's IP addresses.
C. Using Network Access Control Lists to allow/deny traffic based on application IP addresses.
D. Migrating the applications to separate subnets from each other.

Commented [LC550]: ANSWER

Question #91

Legacy applications currently send messages through a single Amazon EC2 instance, which then routes the messages to the appropriate destinations. The Amazon EC2 instance is a bottleneck and single point of failure, so the company would like to address these issues. Which services could address this architectural use case? (Choose two.)

A. Amazon SNS.
B. AWS STS.
C. Amazon SQS.
D. Amazon Route 53.
E. AWS Glue.

Commented [LC551]: ANSWER

Commented [LC552]: ANSWER

Question #92

A Solutions Architect needs to design an architecture for a new, mission-critical batch processing billing application. The application is required to run Monday, Wednesday, and Friday from 5 AM to 11 AM. Which is the MOST cost-effective Amazon EC2 pricing model?

A. Amazon EC2 Spot Instances.
B. On-Demand Amazon EC2 Instances.
C. Scheduled Reserved Instances.
D. Dedicated Amazon EC2 Instances.

Commented [LC553]: ANSWER

Question #93

A workload consists of downloading an image from an Amazon S3 bucket, processing the image, and moving it to another Amazon S3 bucket. An Amazon EC2 instance runs a scheduled task every hour to perform the operation. How should a Solutions Architect redesign the process so that it is highly available?

A. Change the Amazon EC2 instance to compute optimized.
B. Launch a second Amazon EC2 instance to monitor the health of the rest.
C. Trigger a Lambda function when a new object is uploaded.
D. Initially copy the images to an attached Amazon EBS volume.

Commented [LC554]: ANSWER

Question #94

An application is running on an Amazon EC2 instance in a private subnet. The application needs to read and write data onto Amazon Kinesis Data Streams, and corporate policy requires that this traffic should not go to the internet. How can these requirements be met?

A. Configure a NAT gateway in a public subnet and route all traffic to Amazon Kinesis through the NAT gateway.
B. Configure a gateway VPC endpoint for Kinesis and route all traffic to Kinesis through the gateway VPC endpoint.
C. Configure an interface VPC endpoint for Kinesis and route all traffic to Kinesis through the gateway VPC endpoint.
D. Configure an AWS Direct Connect private virtual interface for Kinesis and route all traffic to Kinesis through the virtual interface.

Commented [LC555]: ANSWER

Question #95

A Solutions Architect is building an application that stores object data. Compliance requirements state that the data stored is immutable. Which service meets these requirements?

A. Amazon S3.
B. Amazon Glacier.
C. Amazon EFS.
D. AWS Storage Gateway.

Commented [LC556]: Ref. https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/use-immutable-storage.html

Question #96

A Solutions Architect is designing a shared Amazon S3 bucket where corporate applications will save objects. How can the Architect ensure that when an application uploads an object to the Amazon S3 bucket, the object is encrypted?

A. Set a CORS configuration.
B. Set a bucket policy to encrypt all Amazon S3 objects.
C. Enable default encryption on the bucket.
D. Set permission for users.

Commented [LC557]: ANSWER

Question #97

An application tier currently hosts two web services on the same set of instances, listening on different ports. Which AWS service should a Solutions Architect use to route traffic to the service based on the incoming request path?

A. AWS Application Load Balancer.
B. Amazon CloudFront.
C. Amazon Classic Load Balancer.
D. Amazon Route 53.

Commented [LC558]: ANSWER

Question #98

A data analytics startup company asks a Solutions Architect to recommend an AWS data store options for indexed data. The data processing engine will generate and input more than 64 TB of processed data every day, with item sizes reaching up to 300 KB. The startup is flexible with data storage and is more interested in a database that requires minimal effort to scale with a growing dataset size. Which AWS data store service should the Architect recommend?

A. Amazon RDS.
B. Amazon Redshift.
C. Amazon DynamoDB.
D. Amazon S3.

Commented [LC559]: ANSWER

Question #99

A Solutions Architect needs to allow developers to have SSH connectivity to web servers. The requirements are as follows:

⇨Limit access to users origination from the corporate network. Web servers cannot have SSH access directly from the Internet. Web servers reside in a private subnet.

Which combination of steps must the Architect complete to meet these requirements? (Choose two.)

A. Create a bastion host that authenticates users against the corporate directory.
B. Create a bastion host with security group rules that only allow traffic from the corporate network.
C. Attach an IAM role to the bastion host with relevant permissions.
D. Configure the web servers ' security group to allow SSH traffic from a bastion host.

Commented [LC560]: Necessary to allow the bastion host to communicate within the network's devices

Commented [LC561]: Necessary for connecting to the bastion host via SSH

E. Deny all SSH traffic from the corporate network in the inbound network ACL.

Questions 100-199

Question #100

A Solutions Architect needs to use AWS to implement pilot light disaster recovery for a three-tier web application hosted in an on-premises datacenter. Which solution allows rapid provision of working, fully-scaled production environment?

A. Continuously replicate the production database server to Amazon RDS. Use AWS CloudFormation to deploy the application and any additional servers if necessary.
B. Continuously replicate the production database server to Amazon RDS. Create one application load balancer and register on-premises servers. Configure ELB Application Load Balancer to automatically deploy Amazon EC2 instances for application and additional servers if the on-premises application is down.
C. Use a scheduled Lambda function to replicate the production database to AWS. Use Amazon Route 53 health checks to deploy the application automatically to Amazon S3 if production is unhealthy.
D. Use a scheduled Lambda function to replicate the production database to AWS. Register on-premises servers to an Auto Scaling group and deploy the application and additional servers if production is unavailable.

Commented [LC562]: ANSWER

Question #101

A Solutions Architect notices slower response times from an application. The CloudWatch metrics on the MySQL RDS indicate Read IOPS are high and fluctuate significantly when the database is under load. How should the database environment be re-designed to resolve the IOPS fluctuation?

A. Change the RDS instance type to get more RAM.
B. Change the storage type to Provisioned IOPS.
C. Scale the web server tier horizontally.
D. Split the DB layer into separate RDS instances.

Commented [LC563]: ANSWER

Question #102

A Solutions Architect is designing a solution that can monitor memory and disk space utilization of all Amazon EC2 instances running Amazon Linux and Windows. Which solution meets this requirement?

A. Default Amazon CloudWatch metrics.
B. Custom Amazon CloudWatch metrics.
C. Amazon Inspector resource monitoring.
D. Default monitoring of Amazon EC2 instances.

Commented [LC564]: B is correct. C is wrong because Amazon Inspector tests the network accessibility of your Ec2 instances and the security state of your apps that run on those instances.
D, A are wrong because you can check individually.
To check by group you need a custom metric.

Question #103

A Solutions Architect is creating a new relational database. The Compliance team will use the database, and mandates that data content must be stored across three different Availability Zones. Which of the following options should the Architect Use?

A. Amazon Aurora.
B. Amazon RDS MySQL with Multi-AZ enabled.
C. Amazon DynamoDB.
D. Amazon ElastiCache.

Commented [LC565]: ANSWER

Question #104

A company needs to quickly ensure that all files created in an Amazon S3 bucket in us-east-1 are also available in another bucket in ap-southeast2. Which option represents the SIMPLIEST way to implement this design?

A. Add an S3 lifecycle rule to move any files from the bucket in us-east-1 to the bucket in ap-southeast-2.
B. Create a Lambda function to be triggered for every new file in us-east-1 that copies the file to the bucket in ap-southeast-2.
C. Use SNS to notify the bucket in ap-southeast-2 to create a file whenever the file is created in the bucket in us-east-1.
D. Enable versioning and Configure cross-region replication from the bucket in us-east-1 to the bucket in ap-southeast-2.

Commented [LC566]: ANSWER

Question #105

An organization has a long-running image processing application that runs on Spot Instances that will be terminated when interrupted. A highly available workload must be designed to respond to Spot Instance interruption notices. The solution must include a two-minute warning when there is not enough capacity. How can these requirements be met?

A. Use Amazon CloudWatch Events to invoke an AWS Lambda function that can launch On-Demand Instances.
B. Regularly store data from the application on Amazon DynamoDB. Increase the maximum number of instances in the AWS Auto Scaling group.
C. Manually place a bid for additional Spot Instances at a higher price in the same AWS Region and Availability Zone.
D. Ensure that the Amazon Machine Image associated with the application has the latest configurations for the launch configuration.

Commented [LC567]: ANSWER

Question #106

A company has an Amazon RDS-managed online transaction processing system that has very heavy read and write. The Solutions Architect notices throughput issues with the system. How can the responsiveness of the primary database be improved?

A. Use asynchronous replication for standby to maximize throughput during peak demand.
B. Offload SELECT queries that can tolerate stale data to READ replica.
C. Offload SELECT and UPDATE queries to READ replica.
D. Offload SELECT query that needs the most current data to READ replica.

Commented [LC568]: ANSWER

Question #107

A company is designing a failover strategy in Amazon Route 53 for its resources between two AWS Regions. The company must have the ability to route a user's traffic to the region with least latency, and if both regions are healthy, Route 53 should route traffic to resources in both regions. Which strategy should the Solutions Architect recommend?

A. Configure active-active failover using Route 53 latency DNS records.
B. Configure active-passive failover using Route 53 latency DNS records.
C. Configure active-active failover using Route 53 failover DNS records.
D. Configure active-passive failover using Route 53 failover DNS records.

Commented [LC569]: ANSWER

Ref.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html

Question #108

A company is developing several critical long-running applications hosted on Docker. How should a Solutions Architect design a solution to meet the scalability and orchestration requirements on AWS?

A. Use Amazon ECS and Service Auto Scaling.
B. Use Spot Instances for orchestration and for scaling containers on existing Amazon EC2 instances.
C. Use AWS OpsWorks to launch containers in new Amazon EC2 instances.
D. Use Auto Scaling groups to launch containers on existing Amazon EC2 instances.

Commented [LC570]: ANSWER

Question #109

A Solutions Architect is developing a new web application on AWS. The Architect expects the application to become very popular, so the application must scale to support the load. The Architect wants to focus on software development and deploying new features without provisioning or managing instances. What solution is appropriate?

A. Amazon API Gateway and AWS Lambda.
B. Elastic Load Balancing with Auto Scaling groups and Amazon EC2.
C. Amazon API Gateway and Amazon EC2.
D. Amazon CloudFront and AWS Lambda.

Commented [LC571]: ANSWER

Question #110

A Solutions Architect is deploying a new production MySQL database on AWS. It is critical that the database is highly available. What should the Architect do to achieve this goal with Amazon RDS?

A. Create a read replica of the primary database and deploy it in a different AWS Region.
B. Enable multi-AZ to create a standby database in a different Availability Zone.
C. Enable multi-AZ to create a standby database in a different AWS Region.
D. Create a read replica of the primary database and deploy it in a different Availability Zone.

Commented [LC572]: Answer

Ref. https://aws.amazon.com/it/rds/features/multi-az/

Question #111

An organization designs a mobile application for their customers to upload photos to a site. The application needs a secure login with MFA. The organization wants to limit the initial build time and maintenance of the solution. Which solution should a Solutions Architect recommend to meet the requirements?

A. Use Amazon Cognito Identity with SMS-based MFA.
B. Edit AWS IAM policies to require MFA for all users.
C. Federate IAM against corporate AD that requires MFA.
D. Use Amazon API Gateway and require SSE for photos.

Commented [LC573]: ANSWER

Question #112

A Solutions Architect is designing a solution to monitor weather changes by the minute. The frontend application is hosted on Amazon EC2 instances. The backend must be scalable to a virtually unlimited size, and data retrieval must occur with minimal latency. Which AWS service should the Architect use to store the data and achieve these requirements?

A. Amazon S3.
B. Amazon DynamoDB.
C. Amazon RDS.
D. Amazon EBS.

Commented [LC574]: Host the website on S3 and keep the files there

Question #113

A company hosts a website on premises. The website has a mix of static and dynamic content, but users experience latency when loading static files. Which AWS service can help reduce latency?

A. Amazon CloudFront with on-premises servers as the origin.
B. ELB Application Load Balancer.
C. Amazon Route 53 latency-based routing.
D. Amazon EFS to store and server static files.

Commented [LC575]: You can specify a custom origin for cloudfront.

Ref. https://digitalcloud.training/certification-training/aws-developer-associate/aws-networking-and-content-delivery/amazon-cloudfront/

Question #114

A company wants to analyse all of its sales information aggregated over the last 12 months. The company expects there to be over 10TB of data from multiple sources. What service should be used?

A. Amazon DynamoDB.
B. Amazon Aurora MySQL.
C. Amazon RDS MySQL.
D. Amazon Redshift.

Commented [LC576]: ANSWER

Question #115

A media company has deployed a multi-tier architecture on AWS. Web servers are deployed in two Availability Zones using an Auto Scaling group with a default Auto Scaling termination policy. The web servers' Auto Scaling group currently has 15 instances running. Which instance will be terminated rest during a scale-in operation?

A. The instance with the oldest launch configuration.
B. The instance in the Availability Zone that has most instances.
C. The instance closest to the next billing hour.
D. The oldest instance in the group.

Commented [LC577]: Very tricky question. The order is:

1) Selects the AZ with most instances;
2) Terminates the instance that was launched from the oldest launch template or launch configuration;
3) If the instances were launched from the same launch template or launch configuration, the instance closest to the next billing hour is terminated.

In this situation there are 15 instances across 3 AZs. SINCE it’s not possible to know the distribution among them, the first check is not passed, so the AZ with more instances is killed.

B is the answer.

Question #116

A retail company has sensors placed in its physical retail stores. The sensors send messages over HTTP when customers interact with in-store product displays. A Solutions Architect needs to implement a system for processing those sensor messages; the results must be available for the Data Analysis team. Which architecture should be used to meet these requirements?

A. Implement an Amazon API Gateway to server as the HTTP endpoint. Have the API Gateway trigger an AWS Lambda function to process the messages, and save the results to an Amazon DynamoDB table.
B. Create an Amazon EC2 instance to server as the HTTP endpoint and to process the messages. Save the results to Amazon S3 for the Data Analysis team to download.
C. Use Amazon Route 53 to direct incoming sensor messages to a Lambda function to process the message and save the results to an Amazon DynamoDB table.

Commented [LC578]: ANSWER

D. Use AWS Direct Connect to connect sensors to DynamoDB so that data can be written directly to a DynamoDB table where it can be accessed by the Data Analysis team.

Question #117

A client is migrating a legacy web application to the AWS Cloud. The current system uses an Oracle database as a relational database management system solution. Backups occur every night, and the data is stored on-premises. The Solutions Architect must automate the backups and identity a storage solution while keeping costs low. Which AWS service will meet these requirements?

A. Amazon RDS.
B. Amazon RedShift.
C. Amazon DynamoDB Accelerator.
D. Amazon ElastiCache.

Commented [LC579]: ANSWER

Question #118

A company has an Amazon RDS database backing its production website. The Sales team needs to run queries against the database to track training program effectiveness. Queries against the production database cannot impact performance, and the solution must be easy to maintain. How can these requirements be met?

A. Use an Amazon Redshift database. Copy the product database into Redshift and allow the team to query it.
B. Use an Amazon RDS read replica of the production database and allow the team to query against it.
C. Use multiple Amazon EC2 instances running replicas of the production database, placed behind a load balancer.
D. Use an Amazon DynamoDB table to store a copy of the data.

Commented [LC580]: ANSWER

Question #119

A company must collect temperature data from thousands of remote weather devices. The company must also store this data in a data warehouse to run aggregations and visualizations. Which services will meet these requirements? (Choose two.)

A. Amazon Kinesis Data Firehouse.
B. Amazon SQS.
C. Amazon Redshift.
D. Amazon SNS.
E. Amazon DynamoDB.

Commented [LC581]: ANSWER

Commented [LC582]: ANSWER

Question #120

A company has a legal requirement to store point-in-time copies of its Amazon RDS PostgreSQL database instance in facilities that are at least 200 miles apart. Use of which of the following provides the easiest way to comply with this requirement?

A. Cross-region read replica.
B. Multiple Availability Zone snapshot copy.
C. Multiple Availability Zone read replica.
D. Cross-region snapshot copy.

Commented [LC583]: ANSWER

Question #121

After reviewing their logs, a startup company noticed large, random spikes in traffic to their web application. The company wants to Configure a cost-efficient Auto Scaling solution to support high availability of the web application. Which scaling plan should a Solutions Architect recommend to meet the company's needs?

A. Dynamic.
B. Scheduled.
C. Manual.
D. Lifecycle.

Commented [LC584]: ANSWER

Question #122

To meet compliance standards, a company must have encrypted archival data storage. Data will be accessed infrequently, with lead times well in advance of when archived data must be recovered. The company requires that the storage be secure, durable, and provided at the lowest price per 1 TB of data stored. What type of storage should be used?

A. Amazon S3.
B. Amazon EBS.
C. Amazon Glacier.

Commented [LC585]: ANSWER

D. Amazon EFS.

Question #123

An online company wants to conduct real-time sentiment analysis about its products from its social media channels using SQL. Which of the following solutions has the LOWEST cost and operational burden?

A. Set up a streaming data ingestion application on Amazon EC2 and connect it to a Hadoop cluster for data processing. Send the output to Amazon S3 and use Amazon Athena to analyse the data.
B. Configure the input stream using Amazon Kinesis Data Streams. Use Amazon Kinesis Data Analytics to write SQL queries against the stream.
C. Configure the input stream using Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to send data to an Amazon Redshift cluster, and then query directly against Amazon Redshift.
D. Set up streaming data ingestion application on Amazon EC2 and send the output to Amazon S3 using Kinesis Data Firehose. Use Athena to analyse the data.

Commented [LC586]: Why not Athena?

Athena: run SQL queries on files in S3. Big Data tool for OLAP (Online Analytical Processing). Example use case: you store gigabytes of data in S3 as files (for example parquet, but also JSON, CSV, etc.) and you want to run a query on it. You can have data with all e-store transactions and prepare a summary report at the end of the month.

Kinesis Analytics: run SQL queries on a data stream. It may be a windowed query. Example use case: with a stream of e-store transactions, get the transaction count or summary value over the last hour. The output can be produced every transaction or every minute, so the output is a new stream of (summary) values.

Question #124

An organization must process a stream of large-volume hashtag data in real time and needs to run custom SQL queries on the data to get insights on certain tags. The organization needs this solution to be elastic and does not want to manage clusters. Which of the following AWS services meets these requirements?

A. Amazon Elasticsearch Service.
B. Amazon Athena.
C. Amazon Redshift.
D. Amazon Kinesis Data Analytics.

Commented [LC587]: Same as before.

Question #125

Which requirements must be met in order for a Solutions Architect to specify that an Amazon EC2 instance should stop rather than terminate when its Spot Instance is interrupted? (Choose two.)

A. The Spot Instance request type must be one-time.
B. The Spot Instance request type must be persistent.
C. The root volume must be an Amazon EBS volume.
D. The root volume must be an instance store volume.
E. The launch Configuration is changed.

Commented [LC588]: ANSWER

Commented [LC589]: ANSWER

Question #126

An application hosted on AWS uses object storage for storing internal reports that are accessed daily by the CFO. Currently, these reports are publicly available. How should a Solutions Architect re-design this architecture to prevent unauthorized access to these reports?

A. Encrypt the files on the client side and store the files on Amazon Glacier, then decrypt the reports on the client side.
B. Move the files to Amazon ElastiCache and provide a username and password for downloading the reports.
C. Specify the use of AWS KMS server-side encryption at the time of an object creation on Amazon S3.
D. Store the files on Amazon S3 and use the application to generate S3 pre-signed URLs to users.

Commented [LC590]: ANSWER

Question #127

A Solutions Architect is designing an application on AWS that will connect to the on-premise data center through a VPN connection. The solution must be able to log network traffic over the VPN. Which service logs this network traffic?

A. AWS CloudTrail logs.
B. Amazon VPC flow logs.
C. Amazon S3 bucket logs.
D. Amazon CloudWatch Logs.

Commented [LC591]: ANSWER

Question #128

A company wants to durably store data in 8 KB chunks. The company will access the data once every few months. However, when the company does access the data, it must be done with as little latency as possible. Which AWS service should a Solutions Architect recommend if cost is NOT a factor?

A. Amazon DynamoDB.
B. Amazon EBS Throughput Optimized HDD Volumes.
C. Amazon EBS Cold HDD Volumes.
D. Amazon ElastiCache.

Commented [LC592]: ANSWER

Question #129

A media company has more than 100 TB of data to be stored and retrieved infrequently. However, the company occasionally receives requests for data within an hour. The company needs a low-cost retrieval method to handle the requests. Which service meets this requirement?

A. Amazon S3 Standard.
B. Amazon Glacier standard retrievals.
C. Amazon Glacier bulk retrievals Amazon S3 Standard Infrequent Access.
D. Amazon S3 Standard Infrequent Access.

Commented [LC593]: ANSWER

Question #130

An on-premises database is experiencing significant performance problems when running SQL queries. With 10 users, the lookups are performing as expected. As the number of users increases, the lookups take three times longer than expected to return values to an application. Which action should a Solutions Architect take to maintain performance as the user count increases?

A. Use Amazon SQS.
B. Deploy Multi-AZ RDS MySQL.
C. Configure Amazon RDS with additional read replicas.
D. Migrate from MySQL to RDS Microsoft SQL Server.

Commented [LC594]: ANSWER

Question #131

A team has an application that detects new objects being uploaded into an Amazon S3 bucket. The uploads trigger a Lambda function to write object metadata into an Amazon DynamoDB table and RDS PostgreSQL database. Which action should the team take to ensure high availability?

A. Enable cross-region replication in the Amazon S3 bucket.
B. Create a Lambda function for each Availability Zone the application is deployed in.
C. Enable multi-AZ on the RDS PostgreSQL database.
D. Create a DynamoDB stream for the DynamoDB table.

Commented [LC595]: ANSWER

Question #132

A media company must store 10 TB of audio recordings. Retrieval happens infrequently and requestors agree on an 8-hour turnaround time. What is the MOST cost-effective solution to store the files?

A. Amazon S3 Standard/Infrequent Access (Standard IA).
B. EBS Throughput Optimized HDD (st1).
C. EBS Cold HDD (sc1).
D. Amazon Glacier.

Commented [LC596]: ANSWER

Question #133

A company wants to improve the performance of their web application after receiving customer complaints. An analysis concluded that the same complex database queries were causing increased latency. What should a Solutions Architect recommend to improve the application's performance?

A. Migrate the database to MySQL.
B. Use Amazon RedShift to analyse the queries.
C. Integrate Amazon ElastiCache into the application.
D. Use a Lambda-triggered request to the backend database.

Commented [LC597]: ANSWER

Question #134

Which tool analyses account resources and provides a detailed inventory of changes over time?

A. AWS Config.
B. AWS CloudFormation.
C. Amazon CloudWatch.
D. AWS Service Catalog.

Commented [LC598]: ANSWER.
B, C clearly wrong.
D is wrong because it’s used for other purposes like sharing a catalog of your offerings to your clients.

Question #135

A Solutions Architect is designing a solution that will include a database in Amazon RDS. Corporate security policy mandates that the database, its logs, and its backups are all encrypted. Which is the MOST efficient option to fulfil the security policy using Amazon RDS?

A. Launch an Amazon RDS instance with encryption enabled. Enable encryption for logs and backups.
B. Launch an Amazon RDS instance. Enable encryption for database, logs and backups.
C. Launch an Amazon RDS instance with encryption enabled. Logs and backups are automatically encrypted.
D. Launch an Amazon RDS instance. Enable encryption for backups. Encrypt logs with a database-engine feature.

Commented [LC599]: ANSWER

Question #136

A Solutions Architect is designing a public-facing web application for employees to upload images to their social media account. The application consists of multiple Amazon EC2 instances behind an elastic load balancer, an Amazon S3 bucket where uploaded images are stored, and an Amazon DynamoDB table for storing image metadata. Which AWS service can the Architect use to automate the process of updating metadata in the DynamoDB table upon image upload?

A. Amazon CloudWatch.
B. AWS CloudFormation.
C. AWS Lambda.
D. Amazon SQS.

Commented [LC600]: ANSWER

Question #137

A company's policy requires that all data stored in Amazon S3 is encrypted. The company wants to use the option with the least overhead and does not want to manage any encryption keys. Which of the following options will meet the company's requirements?

A. AWS CloudHSM.
B. AWS Trusted Advisor.
C. Server Side Encryption (SSE-S3).
D. Server Side Encryption (SSE-KMS).

Commented [LC601]: ANSWER

A is wrong because it's for hardware keys
B is wrong because it's a service for checking the security of your account with your advisor
C is correct
D is wrong because you don't want to manage keys

Question #138

A company has gigabytes of web log files stored in an Amazon S3 bucket. A Solutions Architect wants to copy those files into Amazon Redshift for analysis. The company's security policy mandates that data is encrypted at rest both in the Amazon Redshift cluster and the Amazon S3 bucket. Which process will fulfil the security requirements?

A. Enable server-side encryption on the Amazon S3 bucket. Launch an unencrypted Amazon Redshift cluster. Copy the data into the Amazon Redshift cluster.
B. Enable server-side encryption on the Amazon S3 bucket. Copy data from the Amazon S3 bucket into an unencrypted Redshift cluster. Enable encryption on the cluster.
C. Launch an encrypted Amazon Redshift cluster. Copy the data from the Amazon S3 bucket into the Amazon Redshift cluster. Copy data back to the Amazon S3 bucket in encrypted form.
D. Enable server-side encryption on the Amazon S3 bucket. Launch an encrypted Amazon Redshift cluster. Copy the data into the Amazon Redshift cluster.

Commented [LC602]: ANSWER

Question #139

An application runs on Amazon EC2 instances in an Auto Scaling group. When instances are terminated, the Systems Operations team cannot determine the root cause, because the logs reside on the terminated instances are lost. How can the root cause be determined?

A. Use ephemeral volumes to store the log files.
B. Use a scheduled Amazon CloudWatch Event to take regular Amazon EBS snapshots.
C. Use an Amazon CloudWatch agent to push the logs to Amazon CloudWatch Logs.
D. Use AWS CloudTrail to pull the logs from the Amazon EC2 instances.

Commented [LC603]: ANSWER

Question #140

A Solutions Architect is designing a customer order processing application that will likely have high usage spikes. What should the Architect do to ensure that customer orders are not lost before being written to an Amazon RDS database? (Choose two.)

A. Use Amazon CloudFront to deliver the application front end.
B. Use Elastic Load Balancing with a round-robin routing algorithm.
C. Have the orders written into an Amazon SQS queue.
D. Scale the number of processing nodes based on pending order volume.

Commented [LC604]: ANSWER

Commented [LC605]: ANSWER

E. Have a standby Amazon RDS instance in a separate Availability Zone.

Question #141

Employees from several companies use an application once a year during a specific 30-day period. The periods are different for each company. traffic to the application spikes during these 30-day periods. How can the application be designed to handle these traffic spikes?

A. Use an Amazon Route 53 latency routing policy to route traffic to an Amazon EC2 instance with the least lag time.
B. Use Amazon S3 to cache static elements of the website requests.
C. Use an Auto Scaling group to scale the number of EC2 instances to match the site traffic.
D. Use Amazon Cloud Front to serve static assets to decrease the load on the EC2 instances.

Commented [LC606]: ANSWER

Question #142

A restaurant reservation application needs the ability to maintain a waiting list. When a customer tries to reserve a table, and none are available, the customer must be put on the waiting list, and the application must notify the customer when a table becomes free. What service should the Solutions Architect recommend to ensure that the system respects the order in which the customer requests are put onto the waiting list?

A. Amazon SNS.
B. AWS Lambda with sequential dispatch.
C. A FIFO queue in Amazon SQS.
D. A standard queue in Amazon SQS.

Commented [LC607]: ANSWER

Question #143

A Solutions Architect is designing a solution for a dynamic website, 'example.com', that is deployed in two regions: Tokyo, Japan and Sydney, Australia. The Architect wants to ensure that users located in Australia are directed to the website deployed in the Sydney region and users located in Japan are redirected to the website in the Tokyo region when they browse to 'example.com'. Which service should the Architect use to achieve this goal with the LEAST administrative effort?

A. Amazon CloudFront with geolocation routing.
B. Amazon Route 53.
C. Application Load Balancer.
D. Network Load Balancer deployed across multiple regions.

Commented [LC608]: ANSWER

Question #144

A company has a popular multi-player mobile game hosted in its on-premises datacenter. The current infrastructure can no longer keep up with demand and the company is considering a move to the cloud. Which solution should a Solutions Architect recommend as the MOST scalable and cost-effective solution to meet these needs?

A. Amazon EC2 and an Application Load Balancer.
B. Amazon S3 and Amazon CloudFront.
C. Amazon EC2 and Amazon Elastic Transcoder.
D. AWS Lambda and Amazon API Gateway.

Commented [LC609]: A. Amazon EC2 and an Application Load Balancer
D. AWS Lambda and Amazon API Gateway

Remember our core requirement; we're looking for the "MOST scalable and cost-effective". Both of these options allow us to create scalable solutions — so we have some more thinking to pick (A) or (D).
I've made an assumption before I start; the current solution uses an RDBMS database and we'll migrate that over to Amazon RDS — and I've assumed that the reason this isn't mentioned in the problem statement is that we'll end up picking the same solution for the database regardless of option chosen. So all we have to consider is the application logic and its compute requirements.
With EC2, we can create auto-scaling groups and use Spot instances to achieve the "cost-effective".
When considering option (A), we have to pay attention to the original problem statement — the demand has out stripped the infrastructure they can use in their on-premise data center. So that statement tells us that there's a lot of compute currently in-use and demand is increasing. I've inferred, a lot.
Therefore, migrating as-is to EC2 will also require a lot of compute resources — like for like — and while costs can be managed through a combination of Reserved and Spot instances, that much compute is still going to have a price tag with it. We add the cost of the Application Load Balancer on top.
In terms of effort required to migrate the application, moving across to EC2 is likely to require fewer application code changes — it could even "lift and shift".
Next to consider is option (D), which would likely require us to rewrite our code as AWS Lambda functions (although naturally stateless, we can handle state and combine API Gateway with web sockets).
AWS Lambda lets us run our code without provisioning or managing servers, and we only pay for the compute time we consume. It naturally scales up to meet the peak demands, and we don't pay for idle instances.
In terms of costs, as we scale out to the volumes implied in the problem statement, running AWS Lambda is likely to be cheaper than running the equivalent load through a fleet of EC2 instances.
The downside is that we would likely need to re-develop our solution (but not doing so wasn't stated as a constraint — so assume a greenfield).
In conclusion, for the "MOST scalable and cost-effective" solution I'd pick (D) — AWS Lambda and API Gateway.

Question #145

A company has instances in private subnets that require outbound access to the internet. This requires:

A. Assigning a public IP address to the instance.
B. Updating the route table associated with the subnet to point internet traffic through a NAT gateway.
C. Updating the security group associated with the subnet to allow ingress on 0.0.0.0/0.
D. Routing traffic from the instance through a VPC endpoint that has internet access.

Commented [LC610]: ANSWER

Question #146

An organization regularly backs up their application data. The application backups are required to be stored on Amazon S3 for a certain amount of time. The backups should be accessed instantly in the event of a disaster recovery. Which of the following Amazon S3 storage classes would be the MOST cost-effective option to meet the needs of this scenario?

A. Glacier Storage Class.
B. Standard Storage Class.
C. Standard Infrequent Access (IA).
D. Deep Glacier Storage Class.

Commented [LC611]: ANSWER

Question #147

An organization runs an online voting system for a television program. During broadcasts, hundreds of thousands of votes are submitted within minutes and sent to a front-end fleet of auto-scaled Amazon EC2 instances. The EC2 instances push the votes to an RDBMS database. The database is unable to keep up with the front-end connection requests. What is the MOST efficient and cost-effective way of ensuring that votes are processed in a timely manner?

A. Each front-end node should send votes to an Amazon SQS queue. Provision worker instances to read the SQS queue and process the message information into RDBMS database.
B. As the load on the database increases, horizontally-scale the RDBMS database with additional memory-optimized instances. When voting has ended, scale down the additional instances.
C. Re-provision the RDBMS database with larger, memory-optimized instances. When voting ends, re-provision the back-end database with smaller instances.
D. Send votes from each front-end node to Amazon DynamoDB. Provision worker instances to process the votes in DynamoDB into the RDBMS database.

Commented [LC612]: ANSWER

Question #148

An application publishes Amazon SNS messages in response to several events. An AWS Lambda function subscribes to these messages. Occasionally the function will fail while processing a message, so the original event message must be preserved for root cause analysis. What architecture will meet these requirements without changing the work flow?

A. Subscribe an Amazon SQS queue to the Amazon SNS topic and trigger the Lambda function from the queue.
B. Configure Lambda to write failures to an SQS Dead Letter Queue.
C. Configure a Dead Letter Queue for the Amazon SNS topic.
D. Configure the Amazon SNS topic to invoke the Lambda function synchronously.

Commented [LC613]: Answer

Question #149

An application uses an Amazon RDS MySQL cluster for the database layer. Database growth requires periodic resizing of the instance. Currently, administrators check the available disk space manually once a week. How can this process be improved?

A. Use the largest instance type for the database.
B. Use AWS CloudTrail to monitor storage capacity.
C. Use Amazon CloudWatch to monitor storage capacity.
D. Use Auto Scaling to increase storage size.

Commented [LC614]: ANSWER

Question #150

A customer owns a MySQL database that is accessed by various clients who expect, at most, 100ms latency on requests. Once a record is stored in the database, it rarely changed. Clients only access one record at a time. Database access has been increasing exponentially due to increased client demand. The resultant load will soon exceed the capacity of the most expensive hardware available for purchase. The customer wants to migrate to AWS, and is willing to change database systems. Which service would alleviate the database load issue and offer virtually unlimited scalability for the future?

A. Amazon RDS.
B. Amazon DynamoDB.
C. Amazon Redshift.
D. AWS Data Pipeline.

Commented [LC615]: ANSWER

Question #151

A business team requires a structured storage solution to store all of a company's historical sales data. Currently there are 4 TB of data, which will grow to hundreds of terabytes within a few years. The team must be able to regularly run queries against the data using current business intelligence tools. Fast performance is required despite the dataset growth. Which solution should the company use?

A. Amazon Redshift.
B. Amazon Aurora.
C. Amazon DynamoDB.
D. Amazon S3.

Commented [LC616]: ANSWER

Question #152

A prediction process requires access to a trained model that is stored in an Amazon S3 bucket. The process takes a few seconds to process an image and make a prediction. The process is not overly resource-intensive, does not require any specialized hardware, and takes less than 512 MB of memory to run. What would be the MOST effective compute solution for this use case?

A. Amazon ECS.
B. Amazon EC2 Spot instances.
C. AWS Lambda functions.
D. AWS Elastic Beanstalk.

Commented [LC617]: ANSWER

Question #153

An application that runs on an Amazon EC2 instance must make secure calls to Amazon S3 buckets. Which steps can a Solutions Architect take to ensure that the calls are made without exposing credentials?

A. Generate an access key ID and a secret key, and assign an IAM role with least privilege.
B. Create an IAM policy granting access to all services and assign it to the Amazon EC2 instance profile.
C. Create an IAM role granting least privilege and assign it to the Amazon EC2 instance profile.
D. Generate temporary access keys to grant users temporary access to the Amazon EC2 instance.

Commented [LC618]: ANSWER

Question #154

A Solutions Architect needs to design a centralized logging solution for a group of web applications running on Amazon EC2 instances. The solution requires minimal development effort due to budget constraints. Which of the following should the Architect recommend?

A. Create a crontab job script in each instance to push the logs regularly to Amazon S3.
B. Install and Configure Amazon CloudWatch Logs agent in the Amazon EC2 instances.
C. Enable Amazon CloudWatch Events in the AWS Management Console.
D. Enable AWS CloudTrail to map all API calls invoked by the applications.

Commented [LC619]: ANSWER

Question #155

A company is using Amazon S3 as its local repository for weekly analysis reports. One of the company-wide requirements is to secure data at rest using encryption. The company chose Amazon S3 server-side encryption. The company wants to know how the object is decrypted when a GET request is issued. Which of the following answers this question?

A. The user needs to place a PUT request to decrypt the object.
B. The user needs to decrypt the object using a private key.
C. Amazon S3 manages encryption and decryption automatically.
D. Amazon S3 provides a server-side key for decrypting the object.

Commented [LC620]: ANSWER

Question #156

A company is looking for a fully-managed solution to store its players' state information for a rapidly growing game. The application runs on multiple Amazon EC2 nodes, which can scale according to the incoming traffic. The request can be routed to any of the nodes, therefore, the state information must be stored in a centralized database. The players' state information needs to be read with strong consistency and needs conditional updates for any changes. Which service would be MOST cost-effective, and scale seamlessly?

A. Amazon S3.
B. Amazon DynamoDB.
C. Amazon RDS.
D. Amazon Redshift.

Commented [LC621]: ANSWER

Question #157

An application is running on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. Four instances are required to handle a predictable traffic load. The Solutions Architect wants to ensure that the operation is fault-tolerant up to the loss of one Availability Zone. Which is the MOST cost-efficient way to meet these requirements?

A. Deploy two instances in each of three Availability Zones.
B. Deploy two instances in each of two Availability Zones.
C. Deploy four instances in each of two Availability Zones.
D. Deploy one instance in each of three Availability Zones.

Commented [LC622]: ANSWER

Question #158

A Solutions Architect is designing a three-tier web application that includes an Auto Scaling group of Amazon EC2 instances running behind an ELB Classic Load Balancer. The security team requires that all web servers must be accessible only through the Load Balancer, and that none of the web servers are directly accessible from the Internet. How should the Architect meet these requirements?

A. Use a Load Balancer installed on an Amazon EC2 instance.
B. Configure the web servers' security group to deny traffic from the public Internet.
C. Create an Amazon CloudFront distribution in front of the ELB Classic Load Balancer.
D. Configure the web tier security group to allow only traffic from the ELB Classic Load Balancer.

Commented [LC623]: ANSWER

Question #159

A Solutions Architect is designing a web application that will be hosted on Amazon EC2 instances in a public subnet. The web application uses a MySQL database in a private subnet. The database should be accessible to database administrators. Which of the following options should the Architect recommend? (Choose two.)

A. Create a bastion host in a public subnet, and use the bastion host to connect to the database.
B. Log in to the web servers in the public subnet to connect to the database.
C. Perform DB maintenance after using SSH to connect to the NAT Gateway in a public subnet.
D. Create an IPSec VPN tunnel between the customer site and the VPC, and use the VPN tunnel to connect to the database.
E. Attach an Elastic IP address to the database.

Commented [LC624]: ANSWER

Commented [LC625]: ANSWER

Question #160

A web application running on Amazon EC2 instances writes data synchronously to an Amazon DynamoDB table Configured for 60 write capacity units. During normal operation the application writes 50 KB/s to the table, but can scale up to 500 KB/ s during peak hours. The application is currently throttling errors from the DynamoDB table during peak hours. What is the MOST cost-efficient change to support the increased traffic with minimal changes to the application?

A. Use Amazon SQS to manage the write operations to the DynamoDB table.
B. Change DynamoDB table Configuration to 600 write capacity units.
C. Increase the number of Amazon EC2 instances to support the traffic.
D. Configure Amazon DynamoDB Auto Scaling to handle the extra demand.

Commented [LC626]: ANSWER

Question #161

One company wants to share the contents of their Amazon S3 bucket with another company. Security requirements mandate that only the other company's AWS accounts have access to the contents of the Amazon S3 bucket. Which Amazon S3 feature will allow secure access to the Amazon S3 bucket?

A. Bucket policy.
B. Object tagging.
C. CORS configuration.
D. Lifecycle policy.

Commented [LC627]: ANSWER

Question #162

A Solutions Architect is designing a service that must have four Amazon EC2 instances running between 8 AM and 6 PM daily. The service requires one EC2 instance outside of those hours. What is the MOST cost-effective way to provide enough compute?

A. Use one Amazon EC2 Reserved Instance and use an Auto Scaling group to add and remove EC2 instances based on CPU utilization.
B. Use one Amazon EC2 On-Demand instance and use an Auto Scaling group to add and remove EC2 instances based on CPU utilization.
C. Use one Amazon EC2 On-Demand instance and use an Auto Scaling Group scheduled action to add three EC2 Spot instances at 7:30 AM and remove three instances at 6:10 PM.
D. Use one Amazon EC2 Reserved Instance and use an Auto Scaling Group scheduled action to add three EC2 On-Demand instances at 7:30 AM and remove three instances at 6:10 PM.

Commented [LC628]: ANSWER

Question #163

A company plans to use an Amazon VPC to deploy a web application consisting of an elastic load balancer, a fleet of web and application servers, and an Amazon RDS MySQL database that should not be accessible from the Internet. The proposed design must be highly available and distributed over two Availability Zones. What would be the MOST appropriate VPC design for this specific use case?

A. Two public subnets for the elastic load balancer, two public subnets for the web servers, and two public subnets for Amazon RDS.
B. One public subnet for the elastic load balancer, two private subnets for the web servers, and two private subnets for Amazon RDS.
C. One public subnet for the elastic load balancer, one public subnet for the web servers, and one private subnet for the database.
D. Two public subnets for the elastic load balancer, two private subnets for the web servers, and two private subnets for RDS.

Commented [LC629]: ANSWER

Question #164

A workload in an Amazon VPC consists of a single web server launched from a custom AMI. Session state is stored in a database. How should the Solutions Architect modify this workload to be both highly available and scalable?

A. Create a launch Configuration with a desired capacity of two web servers across multiple Availability Zones. Create an Auto Scaling group with the AMI ID of the web server image. Use Amazon Route 53 latency-based routing to balance traffic across the Auto Scaling group.
B. Create a launch Configuration with the AMI ID of the web server image. Create an Auto Scaling group using the newly-created launch configuration, and a desired capacity of two web servers across multiple regions. Use an Application Load Balancer (ALB) to balance traffic across the Auto Scaling group.
C. Create a launch Configuration with the AMI ID of the web server image. Create an Auto Scaling group using the newly-created launch configuration, and a desired capacity of two web servers across multiple Availability Zones. Use an ALB to balance traffic across the Auto Scaling group.
D. Create a launch Configuration with the AMI ID of the web server image. Create an Auto Scaling group using the newly-created launch configuration, and a desired capacity of two web servers across multiple Availability Zones. Use Amazon Route 53 weighted routing to balance traffic across the Auto Scaling group.

Commented [LC630]: ANSWER

Question #165

A Solutions Architect is developing a new web application on AWS. The services must scale to support an increasing load. The Architect wants to focus on software development and deploying new features rather than provisioning or managing servers. Which AWS service is appropriate?

A. Auto Scaling.
B. Elastic Beanstalk.
C. EC2 Container Service.
D. CloudFormation.

Commented [LC631]: ANSWER

Question #166

A company wants to migrate a three-tier web application to AWS. The company wants to control the placement of the instances and have visibility into underlying sockets and cores for licensing purposes. Which compute model should a Solutions Architect choose to accomplish this task?

A. EC2 Reserved Instances.
B. EC2 Spot Instances.
C. EC2 Dedicated Hosts.
D. EC2 Placement Groups.

Commented [LC632]: ANSWER

Question #167

An application runs on multiple Amazon EC2 instances. Each running instance of the application must have access to a shared file system. Where should the data be stored?

A. Amazon S3.
B. Amazon DynamoDB.
C. Amazon EFS.
D. Amazon EBS.

Commented [LC633]: ANSWER

Question #168

A Solutions Architect is designing a microservice to process records from Amazon Kinesis Streams. The metadata must be stored in Amazon DynamoDB. The microservice must be capable of concurrently processing 10,000 records daily as they arrive in the Kinesis stream. The MOST scalable way to design the microservice is:

A. As an AWS Lambda function.
B. As a process on an Amazon EC2 instance.
C. As a Docker container running on Amazon ECS.
D. As a Docker container on an EC2 instance.

Commented [LC634]: ANSWER

Question #169

A university is running an internal web application on AWS that students can access from the university network to check their exam results. The web application runs on Amazon EC2 instances and pulls results from an Amazon DynamoDB table. Auto Scaling is currently Configured to add a new web server when CPU is greater than 80% for 5 minutes. DynamoDB is Configured to increase both read and write capacity units by five when utilization is greater than 80%. Exam results are released at 9:00 a.m. each Monday, and 80% of students, attempt to access their unique result within the rest 30 minutes. Despite Auto Scaling being enabled, students are complaining of slow response times and errors when they view the site. There are no performance complaints after 9:30 a.m. on Monday. Which recommendation should a Solutions Architect make to improve performance in a cost-effective manner?

A. Scale out the EC2 instances to ensure that the environment scales up and down based on the highest load.
B. Implement Amazon DynamoDB Accelerator to improve database performance and remove the need to scale the read/write units.
C. Use a scheduled job to scale out EC2 before 9:00 a.m. on Monday and to scale down after 9:30 a.m.
D. Use Amazon CloudFront to cache web request and reduce the load on EC2 and DynamoDB.

Commented [LC635]: ANSWER

Question #170

As part of a migration strategy, a Solutions Architect needs to analyse workloads that can be optimized for performance and cost. The Solutions Architect has identified a stateless application that serves static content as a potential candidate to move to the cloud. The Solutions Architect has the flexibility to choose an identity solution between Facebook, Twitter, and Amazon. Which AWS solution offers flexibility and ease of use, and the LEAST operational overhead for this migration?

A. Use AWS Identity and Access Management (IAM) for managing identities, and migrate the application to run on Amazon S3, Amazon API Gateway, and AWS Lambda.
B. Use a third-party solution for managing identities, and migrate the application to run on Amazon S3, EC2 Spot Instances, and Amazon EC2.
C. Use Amazon Cognito for managing identities, and migrate the application to run on Amazon S3, Amazon API Gateway, and AWS Lambda.
D. Use Amazon Cognito for managing identities, and migrate the application to run on Amazon S3, EC2 Spot Instances, and Amazon EC2.

Commented [LC636]: ANSWER

Question #171

A company needs to capture all client connection information from its Application Load Balancer every five minutes. This data will be used to analyse traffic patterns and troubleshoot the application. How can a Solutions Architect meet this requirement?

A. Enable AWS CloudTrail for the Application Load Balancer.
B. Enable Access Logs on the Application Load Balancer.
C. Install CloudWatch Agent on the Application Load Balancer.
D. Enable CloudWatch metrics on the Application Load Balancer.

Commented [LC637]: ANSWER

Question #172

An application runs on EC2 instances behind an Elastic Load Balancing Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones. The application provides a RESTful interface with both synchronous and asynchronous operations. The asynchronous operations require up to 5 minutes to complete. Although the application must remain available at all times, after business hours, the traffic going to the application is greatly reduced and often results in the Auto Scaling group running the minimum number of On-Demand Instances. What should the Solutions Architect recommend to optimize the cost of the environment after business hours?

A. Change the Availability Zones in which the instances were created to another Availability Zone in the same region with a lower cost.
B. Replace all On-Demand Instances with Spot Instances in the Auto Scaling group.
C. Purchase Reserved Instances for the minimum number of Auto Scaling instances.
D. Reduce the number of minimum instances to 0. New requests to the Application Load Balancer create new instances.

Commented [LC638]: ANSWER.

Since it keeps running the minimum number and the autoscaling works, a way to reduce the costs is to purchase the minimum number of instances that are always needed, which is 1. So C is the answer.

Question #173

A Solutions Architect is designing a web application for document sharing. The users will upload documents that are then made available to other users. There will be tens of thousands of these documents. What is the MOST cost-effective storage solution?

A. Amazon EFS.
B. Amazon S3.
C. Amazon Glacier.
D. Amazon EBS.

Commented [LC639]: ANSWER

Question #174

A Solutions Architect was tasked with reviewing several templates that build VPCs and ensuring that they meet specific security requirements. After reviewing the templates, the Architect realizes that all of the templates are missing important security best practices. What should the Architect do to implement security best practices in an efficient manner?

A. Use VPC peering to enforce network consistency.
B. Restrict users from deploying an AWS CloudFormation template.
C. Provide the teams a nested AWS CloudFormation template that builds the VPC correctly.
D. Create AWS Identity and Access Management (IAM) policies that enforce the corporate VPC architecture standards.

Commented [LC640]: ANSWER

Question #175

A Solutions Architect has been given the following requirements for a company's VPC:

✑ The solution is a two-tiered application with a web tier and a database tier.

✑ All web traffic to the environment must be directed from the Internet to an Application Load Balancer.

✑ The web servers and the databases should not obtain public IP addresses or be directly accessible from the public Internet.

✑ Because of security requirements, databases may not share a route table or subnet with any other service.

✑ The environment must be highly available within the same VPC for all services.

What is the minimum number of subnets that the Solutions Architect will need based on these requirements and best practices?

A. 2.
B. 3.
C. 4.
D. 6.

Commented [LC641]: ANSWER

Question #176

An application currently stores objects in Amazon S3-Standard. The application accesses new objects frequently for one week. After one week, they are accessed occasionally for analysis batch jobs. A Solutions Architect has been asked to reduce storage costs for the application while allowing immediate access for batch jobs. How can costs be reduced without reducing data durability?

A. Create a lifecycle policy that moves Amazon S3 data to Amazon S3 One Zone-Infrequent Access storage after 7 days. After 30 days, move the data to Amazon Glacier.
B. Keep the data on Amazon S3, and create a lifecycle policy to move S3 data to Amazon Glacier after 7 days.
C. Move all Amazon S3 data to S3 Standard-Infrequent Access storage, and create a lifecycle policy to move the data to Amazon Glacier after 7 days.
D. Keep the data on Amazon S3, then create a lifecycle policy to move the data to S3 Standard-Infrequent Access storage after 7 days.

Commented [LC642]: ANSWER

Question #177

A company is building a critical ingestion service on AWS that will receive 1000 incoming events per second. The events must be processed in order, and no events may be lost. Multiple applications will need to process each event. The company will expose the service as RESTful calls through an API Gateway. What should a Solutions Architect use to receive the events based on these requirements?

A. Amazon Kinesis Data Stream.
B. Amazon DynamoDB.
C. Amazon SQS.
D. Amazon SNS.

Commented [LC643]: ANSWER

Question #178

An AWS Lambda function requires access to an Amazon RDS for SQL Server instance. It is against company policy to store passwords in Lambda functions. How can a Solutions Architect enable the Lambda function to retrieve the database password without violating company policy?

A. Add an IAM policy for IAM database access to the Lambda execution role.
B. Store a one-way hash of the password in the Lambda function.
C. Have the Lambda function use the AWS Systems Manager Parameter Store.
D. Connect to the Amazon RDS for SQL Server instance by using a role assigned to the Lambda function.

Commented [LC644]: ANSWER

Question #179

A company has two different types of reporting needs on their 200-GB data warehouse:

✑ Data scientists run a small number of concurrent ad hoc SQL queries that can take several minutes each to run.

✑ Display screens throughout the company run many fast SQL queries to populate dashboards.

Which design would meet these requirements with the LEAST cost?

A. Replicate relevant data between Amazon Redshift and Amazon DynamoDB. Data scientists use Redshift. Dashboards use DynamoDB.
B. Configure auto-replication between Amazon Redshift and Amazon RDS. Data scientists use Redshift. Dashboards use RDS.
C. Use Amazon Redshift for both requirements, with separate query queues Configured in workload management.
D. Use Amazon Redshift for Data Scientists. Run automated dashboard queries against Redshift and store the results in Amazon ElastiCache. Dashboards query ElastiCache.

Commented [LC645]: ANSWER

Question #180

A company has an application that uses Amazon CloudFront for content that is hosted on an Amazon S3 bucket. After an unexpected refresh, the users are still seeing old content. Which step should the Solutions Architect take to ensure that new content is displayed?

A. Perform a cache refresh on the CloudFront distribution that is serving the content.
B. Perform an invalidation on the CloudFront distribution that is serving the content.
C. Create a new cache behavior path with the updated content.
D. Change the TTL value for removing the old objects.

Commented [LC646]: ANSWER

Question #181

A company expects its user base to increase five times over one year. Its application is hosted in one region and uses an Amazon RDS MySQL database, an ELB Application Load Balancer, and Amazon ECS to host the website and its microservices. Which design changes should a Solutions Architect recommend to support the expected growth? (Choose two.)

A. Move static files from ECS to Amazon S3.
B. Use an Amazon Route 53 geolocation routing policy.
C. Scale the environment based on real-time AWS CloudTrail logs.
D. Create a dedicated Elastic Load Balancer for each microservice.
E. Create RDS read replicas and change the application to use these replicas.

Commented [LC647]: ANSWER

Commented [LC648]: ANSWER

Question #182

A company is rolling out a new web service, but is unsure how many customers the service will attract. However, the company is unwilling to accept any downtime. What could a Solutions Architect recommend to the company in order to keep track of customers' current session data?

A. Amazon EC2.
B. Amazon RDS.
C. AWS CloudTrail.
D. Amazon DynamoDB.

Commented [LC649]: ANSWER

Question #183

A web application is running on Amazon EC2 instances behind an Elastic Load Balancing Application Load Balancer (ALB). The EC2 instances should receive no traffic, except for web requests to the application. Based on these requirements, what security group rules should be put on the Amazon EC2 instances?

A. An inbound rule allowing traffic from the security group attached to the ALB.
B. An inbound rule allowing traffic from the network ACLs attached to the ALB.
C. An outbound rule allowing traffic to the security group attached to the ALB.
D. An outbound rule blocking all traffic to the Internet.

Commented [LC650]: ANSWER

Question #184

A Solutions Architect must migrate a monolithic on-premises application to AWS. It is a web application with a load balancer, web server, application server, and relational database. The key requirement driving the migration is that the application should perform better and be more elastic. Which of the following architectures would meet these requirements?

A. Re-host the application on Amazon EC2 with lift and shift of existing application code. Configure an Elastic Load Balancing load balancer to handle incoming requests. Use Amazon CloudWatch alarms to receive notification of scaling issues. Increase and decrease the size of the Amazon EC2 instances using AWS CLI or AWS Management Console as required.
B. Re-architect the application as a three-tier application. Move the database to Amazon RDS. Use read replicas and Amazon ElastiCache with RDS for better performance. Use an Application Load Balancer to forward incoming requests to web and application servers running on-premises.
C. Re-platform the application as a three-tier application. Use Elastic Load Balancing for incoming requests. Use EC2 for web and application tiers. Use RDS at the database tier. Use CloudWatch alarms and Auto Scaling for horizontal scaling at the web tier.
D. Re-architect the application as Service Oriented Architecture (SOA). Run database and application servers on-premises. Run web-facing EC2 servers. Use an Enterprise Service Bus to handle communications between different parts of the application running on-premises and in the cloud.

Commented [LC651]: ANSWER

Question #185

A company has asked the Solutions Architect to modify its AWS-hosted internal application to allow for load balancing. The customer requests always come from the company domain (example.net). The company requires that incoming HTTP and HTTPS traffic is routed based on the path element of the URL in the request. Which implementation can satisfy all requirements?

A. Configure a Network Load Balancer with listeners for appropriate path patterns for the target groups.
B. Configure an Application Load Balancer with host-based routing based on the domain field in the HTTP header.
C. Configure a Network Load Balancer and enable cross-zone load balancing to ensure that all EC2 instances are used.
D. Configure an Application Load Balancer with listeners for appropriate path patterns for the target group.

Commented [LC652]: ANSWER

Question #186

A Solutions Architect is asked to improve the fault tolerance of an existing Python application. The web application places 1-MB images is an S3 bucket. The application then uses a single t2.large instance to transform the image to include a watermark with the company's brand before writing the image back to the S3 bucket. What should the Solutions Architect recommend to increase the fault tolerance of the solution?

A. Convert the code to a Lambda function triggered by scheduled Amazon CloudWatch Events.
B. Increase the instance size to m4.xlarge and Configure Enhanced Networking.
C. Convert the code to a Lambda function triggered by Amazon S3 events.
D. Create an Amazon SQS queue to send the images to the t2.large instance.

Commented [LC653]: ANSWER

Question #187

A Solutions Architect has been asked to deliver video content stored on Amazon S3 to specific users from Amazon CloudFront while restricting access by unauthorized users. How can the Architect implement a solution to meet these requirements?

A. Configure CloudFront to use signed-URLs to access Amazon S3.
B. Store the videos as private objects in Amazon S3, and let CloudFront serve the objects by using only Origin Access Identity (OAI).
C. Use Amazon S3 static website as the origin of CloudFront, and Configure CloudFront to deliver the videos by generating a signed URL for users.
D. Use OAI for CloudFront to access private S3 objects and select the Restrict Viewer Access option in CloudFront cache behavior to use signed URLs.

Commented [LC654]: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

Question #188

A Solutions Architect needs to deploy a node.js-based web application that is highly available and scales automatically. The Marketing team needs to roll back on application releases quickly, and they need to have an operational dashboard. The Marketing team does not want to manage deployment of OS patches to the Linux servers. Use of which AWS service will satisfy these requirements?

A. Amazon EC2.
B. Amazon API Gateway.
C. AWS Elastic Beanstalk.
D. Amazon EC2 Container Service.

Commented [LC655]: ANSWER

Question #189

A company has a website running on Amazon EC2. The application DNS name points to an Elastic IP address associated with the EC2 instance. In the event of an attack on the website coming from a specific IP address, the company wants a way to block the offending IP address. Which tool or service should a Solutions Architect recommend to block the IP address?

A. Security groups.
B. Network ACL.
C. AWS WAF.
D. AWS Shield.

Commented [LC656]: Since it's only 1, NACL.

Question #190

A customer is looking for a storage archival solution for 1,000 TB of data. The customer requires that the solution be durable and data be available within a few hours of requesting it, but not exceeding a day. The solution should be as cost-effective as possible. To meet security compliance policies, data must be encrypted at rest. The customer expects they will need to fetch the data two times in a year. Which storage solution should a Solutions Architect recommend to meet these requirements?

A. Copy data to Amazon S3 buckets by using server-side encryption. Move data to Amazon S3 to reduce redundancy storage (RRS).
B. Copy data to encrypted Amazon EBS volumes, then store data into Amazon S3.
C. Copy each object into a separate Amazon Glacier vault, and let Amazon Glacier take care of encryption.
D. Copy data to Amazon S3 with server-side encryption. Configure lifecycle management policies to move data to Amazon Glacier after 0 days.

Commented [LC657]: ANSWER

C is wrong, why a single object in a single vault?

Question #191

A web application runs on 10 EC2 instances launched from a single customer Amazon Machine Image (AMI). The EC2 instances are behind an Internet Application Load Balancer. Amazon Route 53 provides DNS for the application. How should a Solutions Architect automate recovery when a web server instance stops replying to request?

A. Launch the instances in an Auto Scaling group with an Elastic Load Balancing health check.
B. Launch instances in multiple Availability Zones and set the load balancer to Multi-AZ.
C. Add CloudWatch alarm actions for each instance to restart if the Status Check (Any) fails.
D. Add Route 53 records for each instance with an instance health check.

Commented [LC658]: ANSWER

Question #192

A company has a Node.js application running on Amazon EC2 that currently retrieves data for customers from a DynamoDB table. The company is seeing many repeat queries for the same items, and the number of queries is continuing to increase as the application gains popularity. What solution will reduce the number of read capacity units (RCUs) required while minimizing the amount of refactoring that must be done to the application?

A. Use Amazon ElastiCache to provide a caching layer.
B. Use a Lambda function to make concurrent requests for caching.
C. Use Amazon DynamoDB Accelerator (DAX) to provide a caching layer.
D. Obtain Reserved Capacity for Amazon DynamoDB to manage the increased number of queries.

Commented [LC659]: ANSWER

Ref. https://aws.amazon.com/it/dynamodb/dax/

Question #193

A company has an application that accesses a MySQL database installed on a single EC2 instance. The instance recently experienced a fault and brought down the entire application for several hours. The company wants to address the issue but is concerned about spending too much time modifying application code or managing the legacy application. What should the Solutions Architect recommend to remove this single point of failure with the FEWEST changes to the application code and the LEAST amount of administrative effort?

A. Implement a caching layer by using Amazon ElastiCache to store query results of frequently accessed information.
B. Deploy a second EC2 instance with MySQL installed, and Configure replication between this instance and the existing MySQL instance.
C. Migrate the database to an RDS MySQL Multi-AZ DB instance, and point the application servers to the new RDS instance.
D. Create a DynamoDB table to use as a cache layer, and update the application to query data from Amazon DynamoDB before querying MySQL.

Commented [LC660]: ANSWER

Question #194

A team is launching a marketing campaign and the peak database read activity in Amazon Aurora for MySQL is expected to increase. A Solutions Architect decides to add two Read Replicas to the cluster. How should the Solutions Architect ensure that the connections for read activities are load balanced?

A. Reader endpoint for Amazon Aurora.
B. Cluster endpoint for Amazon Aurora.
C. Primary DB instance endpoint for Amazon Aurora.
D. Replica DB instances endpoint for Aurora.

Commented [LC661]: ANSWER

Question #195

A company plans to migrate a website to AWS to use a serverless architecture. The website contains both static and dynamic content and is accessed by users across the world. The website should maintain sessions for returning users to improve the user experience. Which service should a Solutions Architect use for a cost-efficient solution with the LOWEST latency?

A. Amazon S3, AWS Lambda, Amazon API Gateway, and Amazon DynamoDB.
B. Amazon CloudFront, AWS Lambda, API Gateway, and Amazon RDS.
C. Amazon CloudFront, Elastic Load Balancing, Amazon EC2, and Amazon RDS.
D. Amazon S3, Amazon CloudFront, AWS Lambda, Amazon API Gateway, and Amazon DynamoDB.

Commented [LC662]: Dynamo for Session Data. S3 + CF for hosting static. Lambda + API Gateway for taking care of dynamic

https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/

Question #196

A Solutions Architect is helping a customer migrate an application to AWS. The application is composed of a fleet of Linux servers that currently use a shared file system to read and write data. One of the goals of moving this application to AWS is to increase the reliability of the storage tier. What solution would increase reliability while minimizing the operational overhead of managing this infrastructure?

A. Create an EBS volume and mount it to all the servers.
B. Create an EFS file system and mount it to all the servers.
C. Create an S3 bucket that can be accessed through an S3 VPC Endpoint.
D. Create two EC2 instances in separate Availability Zones that act as le servers.

Commented [LC663]: ANSWER

Question #197

A Solution Architect is designing a two-tier application for maximum security, with a web tier running on EC2 instances and the data stored in an RDS DB instance. The web tier should accept user access only through HTTPS connections (port 443) from the Internet, and the data must be encrypted in transit to and from the database. What combination of steps will MOST securely meet the stated requirements? (Choose two.)

A. Create a security group for the web tier instances that allows inbound traffic only over port 443.
B. Enforce Transparent Data Encryption (TDE) on the RDS database.
C. Create a network ACL that allows inbound traffic only over port 443.
D. Configure the web servers to communicate with RDS by using SSL, and issue certificates to the web tier EC2 instances.
E. Create a customer master key in AWS KMS and apply it to encrypt the RDS instance.

Commented [LC664]: ANSWER

Commented [LC665]: ANSWER

Question #198

A credit card processing application, hosted on an on-premises server, needs to communicate directly with a database hosted on an Amazon EC2 instance running in a private subnet of a VPC. Compliance requirements state that end-to-end communication should be encrypted. Which solution will ensure that this requirement is met?

A. Use HTTPS for traffic over VPC peering between the VPC and the on-premises datacenter.
B. Use HTTPS for traffic over the Internet between the on-premises server and the Amazon EC2 instance.
C. Use HTTPS for traffic over a VPN connection between the VPC and the on-premises datacenter.
D. Use HTTPS for traffic over gateway VPC endpoints that have been Configured for the Amazon EC2 instance.

Commented [LC666]: ANSWER

Question #199

A company has asked a Solutions Architect to ensure that data is protected during data transfer to and from Amazon S3. Use of which service will protect the data in transit?

A. AWS KMS.
B. HTTPS.
C. SFTP.
D. FTPS.

Commented [LC667]: ANSWER

Questions 200-299

Question #200

A Solutions Architect is trying to bring a data warehouse workload to an Amazon EC2 instance. The data will reside in Amazon EBS volumes and full table scans will be executed frequently. What type of Amazon EBS volume would be most suitable in this scenario?

A. Throughput Optimized HDD (st1).
B. Provisioned IOPS SSD (io1).
C. General Purpose SSD (gp2).
D. Cold HDD (sc1).

Commented [LC668]: Poorly written. A is good enough for full table scans but no data rate is mentioned.

Question #201

A Solutions Architect has a three-tier web application that serves customers worldwide. Analysis reveals that product images take more time to load than expected. Which action will improve the image load time?

A. Store product images on Amazon EBS-optimized storage volumes.
B. Store product images in an Amazon S3 bucket.
C. Use an Amazon CloudFront distribution for product images.
D. Use an Auto Scaling group to add instances for product images.

Commented [LC669]: ANSWER

Question #202

A gaming application is heavily dependent on caching and uses Amazon ElastiCache for Redis. The application performance was recently degraded due to failure of the cache node. What should a Solutions Architect recommend to minimize performance degradation in the future?

A. Migrate from ElastiCache to Amazon RDS.
B. Configure automatic backup to save cache data.
C. Configure ElastiCache Multi-AZ with automatic failover.
D. Use Auto Scaling to provision cache nodes based on CPU usage.

Commented [LC670]: ANSWER

Question #203

A client has set up an Auto Scaling group associated with a load balancer. The client has noticed that instances launched by the Auto Scaling group are reported unhealthy as the result of an Elastic Load Balancing (ELB) health check, but these unhealthy instances are not being terminated. What can a Solutions Architect do to ensure that the instances marked unhealthy will be terminated and replaced?

A. Increase the value for the health check interval set on the ELB load balancer.
B. Change the thresholds set on the Auto Scaling group health check.
C. Change the health check type to ELB for the Auto Scaling group.
D. Change the health check set on the ELB load balancer to use TCP rather than HTTP checks.

Commented [LC671]: I agree with B. C, D clearly wrong. A is wrong because "increasing" makes only the interval longer, giving the instances even more time before getting terminated.

Question #204

A Solutions Architect must review an application deployed on EC2 instances that currently stores multiple 5-GB files on attached instance store volumes. The company recently experienced a significant data loss after stopping and starting their instances and wants to prevent the data loss from happening again. The solution should minimize performance impact and the number of code changes required. What should the Solutions Architect recommend?

A. Store the application data in Amazon S3.
B. Store the application data in an EBS volume.
C. Store the application data in Amazon ElastiCache.
D. Store the application data in Amazon DynamoDB.

Commented [LC672]: ANSWER

Question #205

An organization is deploying Amazon ElastiCache for Redis and requires password protection to improve their data security posture. Which solution should a Solutions Architect recommend?

A. Redis Auth.
B. AWS Single Sign-On.
C. IAM database authentication.
D. VPC security group for Redis.

Commented [LC673]: Ref. https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html

Question #206

A Solutions Architect is designing a solution to send Amazon CloudWatch Alarm notifications to a group of users on a smartphone mobile application. What are the key steps to this solution? (Choose two.)

A. Configure the CloudWatch Alarm to send the notification to an Amazon SNS topic whenever there is an alarm.
B. Configure the CloudWatch Alarm to send the notification to a mobile phone number whenever there is an alarm.
C. Configure the CloudWatch Alarm to send the notification to the email addresses whenever there is an alarm.
D. Create the platform endpoints for mobile devices and subscribe the SNS topic with platform endpoints.
E. Subscribe the SNS topic with an Amazon SQS queue, and poll the messages continuously from the queue. Use each mobile platform's libraries to send the message to the mobile application.

Commented [LC674]: ANSWER

Commented [LC675]: ANSWER

Question #207

A company uses Amazon S3 for storing a variety of files. A Solutions Architect needs to design a feature that will allow users to instantly restore any deleted files within 30 days of deletion. Which is the MOST cost-efficient solution?

A. Create lifecycle policies that move the objects to Amazon Glacier and delete them after 30 days.
B. Enable cross-region replication. Empty the replica bucket every 30 days using an AWS Lambda function.
C. Enable versioning and create a lifecycle policy to remove expired versions after 30 days.
D. Enable versioning and MFA Delete. Using a Lambda function, remove MFA delete from objects more than 30 days old.

Commented [LC676]: ANSWER

Question #208

An application running on Amazon EC2 has been experiencing performance issues when accessing an Amazon RDS for Oracle database. The database has been provisioned correctly for average workloads, but there are several usage spikes each day that have saturated the database, causing the application to time out. The application is write-heavy, updating information more often than reading information. A Solutions Architect has been asked to review the application design. What should the Solutions Architect recommend to improve performance?

A. Put an Amazon ElastiCache cluster in front of the database and use lazy loading to limit database access during peak periods.
B. Put an Amazon Elasticsearch domain in front of the database and use a Write-Through cache to reduce database access during peak periods.
C. Configure an Amazon RDS Auto Scaling group to automatically scale the RDS instance during load spikes.
D. Change the Amazon RDS instance storage type from General Purpose SSD to provisioned IOPS SSD.

Commented [LC677]: ANSWER

Question #209

During performance testing of an application, the Amazon RDS database caused a performance bottleneck. What steps can be taken to improve the database performance? (Choose two.)

A. Change the RDS database instance to multiple Availability Zones.
B. Scale up to a larger RDS instance type.
C. Redirect read queries to RDS read replicas.
D. Scale out using an Auto Scaling group for RDS.
E. Use RDS in a separate AWS Region.

Commented [LC678]: ANSWER

Commented [LC679]: ANSWER

Question #210

A Solutions Architect must design an Amazon DynamoDB table to store data about customer activities. The data is used to analyse recent customer behaviour, so data that is less than a week old is heavily accessed and older data is accessed infrequently. Data that is more than one month old never needs to be referenced by the application, but needs to be archived for year-end analytics. What is the MOST cost-efficient way to meet these requirements? (Choose two.)

A. Use DynamoDB time-to-live settings to expire items after a certain time period.
B. Provision a higher write capacity unit to minimize the number of partitions.
C. Create separate tables for each week's data with higher throughput for the current week.
D. Pre-process data to consolidate multiple records to minimize write operations.
E. Export the old table data from DynamoDB to Amazon S3 using AWS Data Pipeline, and delete the old table.

Commented [LC680]: ANSWER

Commented [LC681]: ANSWER

Question #211

A Solutions Architect is concerned that the current security group rules for a database tier are too permissive and may permit requests that should be restricted. Below are the current security group permissions for the database tier:

⇨ Protocol: TCP

⇨ Port Range: 1433 (MS SQL)

⇨ Source: ALL

Currently, the only identified resource that needs to connect to the databases is the application tier consisting of an Auto Scaling group of EC2 instances. What changes can be made to this security group that would offer the users LEAST privilege?

A. Change the source to -1 to remove source IP addresses previously unseen.
B. Change the source to the VPC CIDR block.
C. Change the source to the application instances IDs.
D. Change the source to the security group ID attached to the application instances.

Commented [LC682]: ANSWER

Question #212

A large media site has multiple applications in Amazon ECS. A Solutions Architect needs to use content metadata and route traffic to specific services. What is the MOST efficient method to perform this task?

A. Use an AWS Classic Load Balancer with a host-based routing option to route traffic to the correct service.
B. Use the AWS CLI to update Amazon Route 53 hosted zone to route traffic as services get updated.
C. Use an AWS Application Load Balancer with host-based routing option to route traffic to the correct service.
D. Use Amazon CloudFront to manage and route traffic to the correct service.

Commented [LC683]: ANSWER

Question #213

A Solutions Architect must build a secure document storage platform that allows clients to access data stored on Amazon S3. Documents must be readily available for the rest 15 days. After that, documents need not be readily available, and storage costs should be reduced as much as possible. Which of the following approaches will satisfy these requirements?

A. Create a lifecycle rule to transition the documents from the STANDARD storage class to the STANDARD_IA storage class after 15 days, and then to the GLACIER storage class after an additional 15 days.
B. Create a lifecycle rule to transition the documents from the STANDARD storage class to the GLACIER storage class after 30 days.
C. Create a lifecycle rule to transition documents from the STANDARD storage class to the STANDARD_IA storage class after 30 days and then to the GLACIER storage class after an additional 30 days.
D. Create a lifecycle rule to transition the documents from the STANDARD storage class to the GLACIER storage class after 15 days.

Commented [LC684]: ANSWER

Question #214

A Solutions Architect needs to Configure scaling policies based on Amazon CloudWatch metrics for an Auto Scaling group. The application running on the instances is memory intensive. How can the Architect meet this requirement?

A. Enable detailed monitoring on the Amazon EC2 instances.
B. Publish custom metrics to CloudWatch from the application.
C. Configuration lifecycle policies for the Amazon EC2 instances.
D. Set up high-resolution alarms for the Auto Scaling group.

Commented [LC685]: ANSWER

Question #215

A customer has a service based out of Oregon, U.S. and Paris, France. The application is storing data in an S3 bucket located in Oregon, and that data is updated frequently. The Paris office is experiencing slow response times when retrieving objects. What should a Solutions Architect do to resolve the slow response times for the Paris office?

A. Set up an S3 bucket based in Paris, and enable cross-region replication from the Oregon bucket to the Paris bucket.
B. Create an Application Load Balancer that load balances data retrieval between the Oregon S3 bucket and a new Paris S3 bucket.
C. Create an Amazon CloudFront distribution with the bucket located in Oregon as the origin and set the Maximum Time to Live (TTL) for cache behavior to 0.
D. Set up an S3 bucket based in Paris, and enable a lifecycle management rule to transition data from the Oregon bucket to the Paris bucket.

Commented [LC686]: ANSWER

Question #216

A company uses AWS Elastic Beanstalk to deploy a web application running on c4.large instances. Users are reporting high latency and failed requests. Further investigation reveals that the EC2 instances are running at or near 100% CPU utilization. What should a Solutions Architect do to address the performance issues?

A. Use time-based scaling to scale the number of instances based on periods of high load.
B. Modify the scaling triggers in Elastic Beanstalk to use the CPUUtilization metric.
C. Swap the c4.large instances with the m4.large instance type.
D. Create an additional Auto Scaling group, and Configure Amazon EBS to use both Auto Scaling groups to increase the scaling capacity.

Commented [LC687]: ANSWER

Question #217

A Solutions Architect is working on a PCI-compliant architecture that needs to call an external service provider's API. The external provider requires IP whitelisting to verify the calling party. How should the Solutions Architect provide the external party with the IP addresses for whitelisting?

A. Use an API Gateway in proxy mode, and provide the API Gateway's IP address to the external service provider.
B. Associate a public elastic network interface to a published stage/endpoint in API Gateway, exposing the AWS Lambda function, and provide the IP address for the public network interface to the external party to whitelist.
C. Deploy the Lambda function in private subnets and route outbound traffic through a NAT gateway. Provide the NAT gateway's Elastic IP address to the external service provider.
D. Provide the external party the allocated AWS IP address range for Lambda functions, and send change notifications by using a subscription to the AmazonIpSpaceChanged SNS topic.

Commented [LC688]: ANSWER

Question #218

A Solutions Architect is designing a shared file system for a company. Multiple users will be accessing it at any given time. Different teams will have their own directories, and the company wants to secure files so that users can access only files owned by their team. How should the Solutions Architect design this?

A. Use Amazon EFS and control permissions by using file-level permissions.
B. Use Amazon S3 and control permissions by using ACLs.
C. Use Amazon EFS and control permissions by using security groups.
D. Use AWS Storage Gateway and control permissions by using AWS Identity and Access Management (IAM).

Commented [LC689]: ANSWER

Question #219

A company requires operating system permission on a relational database server. What should a Solutions Architect suggest as a Configuration for a highly available database architecture?

A. Multiple EC2 instances in a database replication Configuration that uses two Availability Zones.
B. A standalone Amazon EC2 instance with a selected database installed.
C. Amazon RDS in a Multi-AZ Configuration with Provisioned IOPS.
D. Multiple EC2 instances in a replication Configuration that uses two placement groups.

Commented [LC690]: Tricky! It's not RDS. It's a Server with a DB installed. So classic HA configuration, I'd go with A.

As a suggestion, the text in C says "Provisioned IOPS" that lets you understand that the answer is wrong.

Question #220

An application has a web tier that runs on EC2 instances in a public subnet. The application tier instances run in private subnets across two Availability Zones. All traffic is IPv4 only, and each subnet has its own custom route table. A new feature requires that application tier instances can call an external service over the Internet; however, they must still not be accessible to Internet traffic. What should be done to allow the application servers to connect to the Internet, maintain high availability, and minimize administrative overhead?

A. Add an Amazon egress-only internet gateway to each private subnet. Alter each private subnet's route table to include a route from 0.0.0.0/0 to the egress-only internal gateway in the same Availability Zone.
B. Add an Amazon NAT Gateway to each public subnet. Alter each private subnet's route table to include a route from 0.0.0.0/0 to the NAT Gateway in the same Availability Zone.
C. Add an Amazon NAT instance to one of the public subnets Alter each private subnet's route table to include a route from 0.0.0.0/0 to the Internet gateway in the VPC.
D. Add an Amazon NAT Gateway to each private subnet. Alter each private subnet's route table to include a route from 0.0.0.0/0 to the NAT Gateway in the other Availability Zone.

Commented [LC691]: ANSWER

Question #221

An application uses an Amazon SQS queue as a transport mechanism to deliver data to a group of EC2 instances for processing. The application owner wants to add a mechanism to archive the incoming data without modifying application code on the EC2 instances. How can this application be re-architected to archive the data without modifying the processing instances?

A. Trigger a Lambda function by using Amazon CloudWatch Events to retrieve messages from the SQS queue and archive to Amazon S3.
B. Use an Amazon SNS topic to fan out the data to the SQS queue in addition to a Lambda function that records the data to an S3 bucket.
C. Set up an Amazon Kinesis Data Stream so that multiple instances can receive data. Add a separate EC2 instance that is Configured to archive all data it receives.
D. Write the data to an S3 bucket, and use an SQS queue for S3 event notifications to tell the instances where to retrieve the data.

Commented [LC692]: ANSWER

Question #222

A Solutions Architect must select the most cost-efficient client architecture for a service that responds to web requests. These web requests are small and query a DynamoDB table. The request rate ranges from zero to several hundred each second, without any predictable patterns. What is the MOST cost-efficient architecture for this service?

A. Network Load Balancer/Amazon EC2.
B. Application Load Balancer/Amazon ECS.
C. API Gateway/AWS Lambda.
D. AWS Elastic Beanstalk/AWS Lambda.

Commented [LC693]: ANSWER

Question #223

A company has a web application running in a Docker container that connects to a MySQL server in an on-premises data center. The deployment and maintenance of this application are becoming time-consuming and slowing down new feature releases. The company wants to migrate the application to AWS and use services that helps facilitate infrastructure management and deployment. Which architectures should the company consider on AWS? (Choose two.)

A. Amazon ECS for the web application, and an Amazon RDS for MySQL for the database.
B. AWS Elastic Beanstalk Docker Multi-container either for the web application or database.
C. AWS Elastic Beanstalk Docker Single Container for the web application, and an Amazon RDS for MySQL for the database.
D. AWS CloudFormation with Lambda Custom Resources without VPC for the web application, and an Amazon RDS for MySQL database.
E. AWS CloudFormation with Lambda Custom Resources running in a VPC for the web application, and an Amazon RDS for MySQL database.

Commented [LC694]: ANSWER

Commented [LC695]: ANSWER

Question #224

A Solutions Architect has designed a VPC that meets all necessary security requirements for their organization. Any applications deployed in the organization must use this VPC design. How can project teams deploy, manage, and delete VPCs that meet this design with the LEAST administrative effort?

A. Deploy an AWS CloudFormation template that defines components of the VPC.
B. Run a script that uses the AWS Command Line Interface to deploy the VPC.
C. Clone the existing authorized VPC for each new project.
D. Use AWS Elastic Beanstalk to deploy both the VPC and the application.

Commented [LC696]: ANSWER

Question #225

What conditions could cause a Multi-AZ Amazon RDS failover to occur? (Choose two.)

A. The RDS instance is stopped manually.
B. A replica of the RDS instance is created in a different region.
C. An Availability Zone becomes unavailable.
D. Another master user is created.
E. A failure of the primary database instance.

Commented [LC697]: ANSWER

Commented [LC698]: ANSWER

Question #226

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB). Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Commented [LC699]: ANSWER

Question #227

A Solutions Architect has five web servers serving requests for a domain. Which of the following Amazon Route 53 routing policies can distribute traffic randomly among all healthy web servers?

A. Simple.
B. Failover.
C. Weighted.
D. Multivalue Answer.

Commented [LC700]: ANSWER

Ref.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/traffic-policies.html

Question #228

A web server will be provisioned on two Amazon EC2 instances with an Application Load Balancer. Which of the following configurations will allow traffic on HTTP and HTTPS when configuring a security group to apply to each of these servers?

A. Allow all inbound traffic, with explicit denies on non-HTTP and non-HTTPS ports.
B. Allow incoming traffic to HTTP and HTTPS ports.
C. Allow incoming traffic to HTTP and HTTPS ports, with explicit denies to all other ports.
D. Deny all traffic to non-HTTP and non-HTTPS ports.

Commented [LC701]: ANSWER

Question #229

A company wants to run a static website served through Amazon CloudFront. What is an advantage of storing the website content in an S3 bucket instead of an EBS volume?

A. S3 buckets are replicated globally, allowing for large scalability. EBS volumes are replicated only within a region.
B. S3 is an origin for CloudFront. EBS volumes would need EC2 instances behind an Elastic Load Balancing load balancer to be an origin.
C. S3 buckets can be encrypted, allowing for secure storage of the web files. EBS volumes cannot be encrypted.
D. S3 buckets support object-level read throttling, preventing abuse. EBS volumes do not provide object-level throttling.

Commented [LC702]: ANSWER

Question #230

A company is moving to AWS. Management has identified a set of approved AWS services that meet all deployment requirements. The company would like to restrict access to all other unapproved services to which employees would have access. Which solution meets these requirements with the LEAST amount of operational overhead?

A. Configure the AWS Trusted Advisor service utilization compliance report. Subscribe to Amazon SNS notifications from Trusted Advisor. Create a custom AWS Lambda function that can automatically remediate the use of unauthorized services.
B. Use AWS Config to evaluate the Configuration settings of AWS resources. Subscribe to Amazon SNS notifications from AWS Config. Create a custom AWS Lambda function that can automatically remediate the use of unauthorized services.
C. Configure AWS Organizations. Create an organizational unit (OU) and place all AWS accounts into the OU. Apply a service control policy (SCP) to the OU that denies the use of certain services.
D. Create a custom AWS IAM policy. Deploy the policy to each account using AWS CloudFormation StackSets. Include deny statements in the policy to restrict the use of certain services. Attach the policies to all IAM users in each account.

Commented [LC703]: ANSWER

Question #231

A customer is running a critical payroll system in a production environment in one data center and a disaster recovery (DR) environment in another region. The application includes load-balanced web servers and failover for the MySQL database. The customer's DR process is manual and error-prone. For this reason, management has asked IT to migrate the application to AWS and make it highly available so that IT no longer has to manually fail over the environment. How should a Solutions Architect migrate the system to AWS?

A. Migrate the production and DR environments to different Availability Zones within the same region. Let AWS manage failover between the environments.
B. Migrate the production and DR environments to different regions. Let AWS manage failover between the environments.
C. Migrate the production environment to a single Availability Zone, and set up instance recovery for Amazon EC2. Decommission the DR environment because it is no longer needed.
D. Migrate the production environment to span multiple Availability Zones, using Elastic Load Balancing and Multi-AZ Amazon RDS. Decommission the DR environment because it is no longer needed.

Commented [LC704]: ANSWER

Question #232

A company is creating a web application that will run on an Amazon EC2 instance. The application on the instance needs access to an Amazon DynamoDB table for storage. What should be done to meet these requirements?

A. Create another AWS account root user with permissions to the DynamoDB table.
B. Create an IAM role and assign the role to the EC2 instance with permissions to the DynamoDB table.
C. Create an identity provider and assign the identity provider to the EC2 instance with permissions to the DynamoDB table.
D. Create identity federation with permissions to the DynamoDB table.

Commented [LC705]: ANSWER

Question #233

A company is creating a web application that allows customers to view photos in their web browsers. The website is hosted in us-east-1 on Amazon EC2 instances behind an Application Load Balancer. Users will be located in many places around the world. Which solution should provide all users with the fastest photo viewing experience?

A. Implement an AWS Auto Scaling group for the web server instances behind the Application Load Balancer.
B. Enable Amazon CloudFront for the website and specify the Application Load Balancer as the origin.
C. Move the photos into an Amazon S3 bucket and enable static website hosting.
D. Enable Amazon ElastiCache in the web server subnet.

Commented [LC706]: ANSWER

Question #234

A Solutions Architect is designing a highly available web application on AWS. The data served on the website is dynamic and is pulled from Amazon DynamoDB. All users are geographically close to one another. How can the Solutions Architect make the application highly available?

A. Host the website data on Amazon S3 and set permissions to enable public read-only access for users.
B. Host the web server data on Amazon CloudFront and update the objects in the Cloudfront distribution when they change.
C. Host the application on EC2 instances across multiple Availability Zones. Use an Auto Scaling group coupled with an Application Load Balancer.
D. Host the application on EC2 instances in a single Availability Zone. Replicate the EC2 instances to a separate region, and use an Application Load Balancer for high availability.

Commented [LC707]: ANSWER

Question #235

A company is migrating on-premises databases to AWS. The company's backend application produces a large amount of database queries for reporting purposes, and the company wants to offload some of those reads to Read Replica, allowing the primary database to continue performing efficiently. Which AWS database platforms will accomplish this? (Select TWO.)

A. Amazon RDS for Oracle.
B. Amazon RDS for PostgreSQL.
C. Amazon RDS for MariaDB.
D. Amazon DynamoDB.
E. Amazon RDS for Microsoft SQL Server.

Commented [LC708]: Up to now, it’s actually three. Probably at the time the answers were only two.

Ref.
https://aws.amazon.com/it/rds/features/read-replicas/

Question #236

An application launched on Amazon EC2 instances needs to publish personally identifiable information (PII) about customers using Amazon SNS. The application is launched in private subnets within an Amazon VPC. Which is the MOST secure way to allow the application to access service endpoints in the same region?

A. Use an internet gateway.
B. Use AWS PrivateLink.
C. Use a NAT gateway.
D. Use a proxy instance.

Commented [LC709]: ANSWER

Question #237

A data-processing application runs on an i3.large EC2 instance with a single 100 GB EBS gp2 volume. The application stores temporary data in a small database (less than 30 GB) located on the EBS root volume. The application is struggling to process the data fast enough, and a Solutions Architect has determined that the I/O speed of the temporary database is the bottleneck. What is the MOST cost-efficient way to improve the database response times?

A. Enable EBS optimization on the instance and keep the temporary files on the existing volume.
B. Put the temporary database on a new 50-GB EBS gp2 volume.
C. Move the temporary database onto instance storage.
D. Put the temporary database on a new 50-GB EBS io1 volume with a 3-K IOPS provision.

Commented [LC710]: ANSWER

Question #238

An application stores data in an Amazon RDS PostgreSQL Multi-AZ database instance. The ratio of read requests to write requests is about 2 to 1. Recent increases in traffic are causing very high latency. How can this problem be corrected?

A. Create a similar RDS PostgreSQL instance and direct all traffic to it.
B. Use the secondary instance of the Multiple Availability Zone for read traffic only.
C. Create a read replica and send half of all traffic to it.
D. Create a read replica and send all read traffic to it.

Commented [LC711]: ANSWER

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

Question #239

A Solutions Architect is designing a system that will store Personally Identifiable Information (PII) in an Amazon S3 bucket. Due to compliance and regulatory requirements, both the master keys and unencrypted data should never be sent to AWS. What Amazon S3 encryption technique should the Architect choose?

A. Amazon S3 client-side encryption with an AWS KMS-managed customer master key (CMK).
B. Amazon S3 server-side encryption with an AWS KMS-managed key.
C. Amazon S3 client-side encryption with a client-side master key.
D. Amazon S3 server-side encryption with a customer-provided key.

Commented [LC712]: ANSWER

Question #240

A Security team reviewed their company's VPC Flow Logs and found that traffic is being directed to the internet. The application in the VPC uses Amazon EC2 instances for compute and Amazon S3 for storage. The company's goal is to eliminate internet access and allow the application to continue to function. What change should be made in the VPC before updating the route table?

A. Create a NAT gateway for Amazon S3 access.
B. Create a VPC endpoint for Amazon S3 access.
C. Create a VPC endpoint for Amazon EC2 access.
D. Create a NAT gateway for Amazon EC2 access.

Commented [LC713]: ANSWER

Question #241

A company is deploying a reporting application on Amazon EC2. The application is expected to generate 1,000 documents every hour and each document will be 800 MB. The company is concerned about strong data consistency and file locking, as various applications hosted on other EC2 instances will process the report documents in parallel when they become available. What storage solution will meet these requirements with the LEAST amount of administrative overhead?

A. Amazon EFS.
B. Amazon S3.
C. Amazon ElastiCache.
D. Amazon EBS.

Commented [LC714]: ANSWER

Question #242

A Solutions Architect is building a WordPress-based web application hosted on AWS using Amazon EC2. This application serves as a blog for an international internet security company. The application must be geographically redundant and scalable. It must separate the public Amazon EC2 web servers from the private Amazon RDS database, it must be highly available, and it must support dynamic port routing. Which combination of AWS services or capabilities will meet these requirements?

A. AWS Auto Scaling with a Classic Load Balancer, and AWS CloudTrail.
B. Amazon Route 53, Auto Scaling with an Application Load Balancer, and Amazon CloudFront.
C. A VPC, a NAT gateway and Auto Scaling with a Network Load Balancer.
D. CloudFront, Route 53, and Auto Scaling with a Classic Load Balancer.

Commented [LC715]: ANSWER

Question #243

An e-commerce application places orders in an Amazon SQS queue. When a message is received, Amazon EC2 worker instances process the request. The EC2 instances are in an Auto Scaling group. How should the architecture be designed to scale up and down with the LEAST amount of operational overhead?

A. Use an Amazon CloudWatch alarm on the EC2 CPU to scale the Auto Scaling group up and down.
B. Use an EC2 Auto Scaling health check for messages processed on the EC2 instances to scale up and down.
C. Use an Amazon CloudWatch alarm based on the number of visible messages to scale the Auto Scaling group up or down.
D. Use an Amazon CloudWatch alarm based on the CPU to scale the Auto Scaling group up or down.

Commented [LC716]: ANSWER

Question #244

A customer is migrating to AWS and requires applications to access Network File System shares without code changes. Data is critical and accessed frequently. Which storage solution should a Solutions Architect recommend to maximize availability and durability?

A. Amazon EBS.
B. Amazon S3.
C. AWS Storage Gateway for files.
D. Amazon EFS.

Commented [LC717]: ANSWER. C is wrong because it doesn't ask for a migration tool.

Question #245

A company has many applications on Amazon EC2 instances running in Auto Scaling groups. Company policies require that data on the attached Amazon EBS volume must be retained. Which actions will meet this requirement without impacting performance?

A. Enable Termination Protection on the Amazon EC2 instances.
B. Disable DeleteOnTermination for the Amazon EBS volumes.
C. Use Amazon EC2 user data to set up a synchronization job for root volume data.
D. Change the auto scaling Health Check to point to a source on the root volume.

Commented [LC718]: ANSWER

Question #246

A company wants to expand its web services from us-east-1 into ap-southeast-1. The company stores a large amount of static content on its website, and recently received complaints about slow loading speeds and the website timing out. What should be done to meet the expansion goal while also addressing the latency and timeout issues?

A. Store the static content in Amazon S3 and enable S3 Transfer Acceleration.
B. Store the static content in an Amazon EBS volume in the ap-southeast-1 region and provision larger Amazon EC2 instances for the website.
C. Use an Amazon Route 53 simple routing policy to distribute cached content across three regions.
D. Use Amazon S3 to store the static content and Configure an Amazon CloudFront distribution.

Commented [LC719]: ANSWER

Question #247

An application is scanning an Amazon DynamoDB table that was created with default settings. The application occasionally reads stale data when it queries the table. How can this issue be corrected?

A. Increase the provisioned read capacity of the table.
B. Enable AutoScaling on the DynamoDB table.
C. Update the application to use strongly consistent reads.
D. Re-create the DynamoDB table with eventual consistency disabled.

Commented [LC720]: ANSWER

Question #248

A company is setting up a new website for online sales. The company will have a web tier and a database tier. The web tier consists of load balanced, auto-scaled Amazon EC2 instances in multiple Availability Zones (AZs). The database tier is an Amazon RDS Multi-AZ deployment. The EC2 instances must connect securely to the database. How should the resources be launched?

A. EC2 instances: public subnet RDS database instances: public subnet Load balancer: public subnet.
B. EC2 instances: public subnet RDS database instances: private subnet Load balancer: private subnet.
C. EC2 instances: private subnet RDS database instances: public subnet Load balancer: public subnet.
D. EC2 instances: private subnet RDS database instances: private subnet Load balancer: public subnet.

Commented [LC721]: ANSWER

Question #249

A customer set up an Amazon VPC with one private subnet and one public subnet with a NAT gateway. The VPC will contain a group of Amazon EC2 instances. All instances will Configure themselves at startup by downloading a bootstrap script from an Amazon S3 bucket with a policy that only allows access from the customer's Amazon EC2 instances and then deploys an application through GIT. A Solutions Architect has been asked to design a solution that provides the highest level of security regarding network connectivity to the Amazon EC2 instances. How should the Architect design the infrastructure?

A. Place the Amazon EC2 instances in the public subnet, with no EIPs; route outgoing traffic through the internet gateway.
B. Place the Amazon EC2 instances in a public subnet, and assign EIPs; route outgoing traffic through the NAT gateway.
C. Place the Amazon EC2 instances in a private subnet, and assign EIPs; route outgoing traffic through the internet gateway.
D. Place the Amazon EC2 instances in a private subnet, with no EIPs; route outgoing traffic through the NAT gateway.

Commented [LC722]: ANSWER

Question #250

A company processed 10 TB of raw data to generate quarterly reports. Although it is unlikely to be used again, the raw data needs to be preserved for compliance and auditing purposes. What is the MOST cost-effective way to store the data in AWS?

A. Amazon EBS Cold HDD (sc1).
B. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).
C. Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
D. Amazon Glacier.

Commented [LC723]: ANSWER

Question #251

A Solutions Architect needs to design a solution that will allow Website Developers to deploy static web content without managing server infrastructure. All web content must be accessed over HTTPS with a custom domain name. The solution should be scalable as the company continues to grow. Which of the following will provide the MOST cost-effective solution?

A. Amazon EC2 instance with Amazon EBS.
B. AWS Lambda function with Amazon API Gateway.
C. Amazon CloudFront with an Amazon S3 bucket origin.
D. Amazon S3 with a static website.

Commented [LC724]: ANSWER

Question #252

A company is running a series of national TV campaigns. These 30-second advertisements will introduce sudden traffic peaks targeted at a Node.js application. The company expects traffic to increase from five requests each minute to more than 5,000 requests each minute. Which AWS service should a Solutions Architect use to ensure traffic surges can be handled?

A. AWS Lambda.
B. Amazon ElastiCache.
C. Size EC2 instances to handle peak load.
D. An Auto Scaling group for EC2 instances.

Commented [LC725]: ANSWER

Question #253

An insurance company stores all documents related to annual policies for the duration of the policies. The documents are created once and then stored until they are required, typically at the end of the policy. A document must be capable of being retrieved immediately. The company is now moving their document management to the AWS Cloud. Which service should a Solutions Architect recommend as a cost-effective solution that meets the company's requirements?

A. Amazon RDS MySQL.
B. Amazon S3 Standard-Infrequent Access.
C. Amazon Glacier.

Commented [LC726]: ANSWER. Glacier is wrong because data needs to be retrieved immediately. A is wrong because it's files.

D. Amazon S3 Standard.

Question #254

How can a user track memory usage in an EC2 instance?

A. Call Amazon CloudWatch to retrieve the memory usage metric data that exists for the EC2 instance.
B. Assign an IAM role to the EC2 instance with an IAM policy granting access to the desired metric.
C. Use an instance type that supports memory usage reporting to a metric by default.
D. Place an agent on the EC2 instance to push memory usage to an Amazon CloudWatch custom metric.

Commented [LC727]: ANSWER

Question #255

A Solutions Architect must design a storage solution for incoming billing reports in CSV format. The data does not need to be scanned frequently and is discarded after 30 days. Which service will be MOST cost-effective in meeting these requirements?

A. Import the logs into an RDS MySQL instance.
B. Use AWS Data Pipeline to import the logs into a DynamoDB table.
C. Write the files to an S3 bucket and use Amazon Athena to query the data.
D. Import the logs to an Amazon Redshift cluster.

Commented [LC728]: ANSWER

Question #256

A Solutions Architect needs to deploy an HTTP/HTTPS service on Amazon EC2 instances with support for WebSockets using load balancers. How can the Architect meet these requirements?

A. Configure a Network Load Balancer.
B. Configure an Application Load Balancer.
C. Configure a Classic Load Balancer.
D. Configure a Layer-4 Load Balancer.

Commented [LC729]: ANSWER

Question #257

A Solution Architect is designing a web application that runs on Amazon EC2 instances behind a load balancer. All data in transit must be encrypted. Which solutions will meet the encryption requirement? (Select TWO.)

A. Use an Application Load Balancer (ALB) in passthrough mode, then terminate SSL on EC2 instances.
B. Use an Application Load Balancer (ALB) with a TCP listener, then terminate SSL on EC2 instances.
C. Use a Network Load Balancer (NLB) with a TCP listener, then terminate SSL on EC2 instances.
D. Use an Application Load Balancer (ALB) with an HTTPS listener, then install SSL certificates on the ALB and EC2 instances.
E. Use a Network Load Balancer (NLB) with an HTTPS listener, then install SSL certificates on the NLB and EC2 instances.

Commented [LC730]: ANSWER

Commented [LC731]: ANSWER

Question #258

A user is designing a new service that receives location updates from 3,600 rental cars every hour. The cars upload their location to an Amazon S3 bucket. Each location must be checked for distance from the original rental location. Which services will process the updates and automatically scale?

A. Amazon EC2 and Amazon EBS.
B. Amazon Kinesis Firehose and Amazon S3.
C. Amazon ECS and Amazon RDS.
D. Amazon S3 events and AWS Lambda.

Commented [LC732]: ANSWER

Question #259

A company is writing a new service running on Amazon EC2 that must create thumbnail images of thousands of images in a large archive. The system will write scratch data to storage during the process. Which storage service is best suited for this scenario?

A. EC2 instance store.
B. Amazon EFS.
C. Amazon CloudSearch.
D. Amazon EBS Throughput Optimized HDD (st1).

Commented [LC733]: Since it's scratch data, it's temporary.

Question #260

A company's Amazon RDS MySQL DB instance may be rebooted for maintenance and to apply patches. This database is critical and potential user disruption must be minimized. What should the Solution Architect do in this scenario?

A. Set up an RDS MySQL cluster.
B. Create an RDS MySQL Read Replica.
C. Set RDS MySQL to Multi-AZ.
D. Create an Amazon EC2 instance MySQL cluster.

Commented [LC734]: ANSWER

Question #261

A retail company operates an e-commerce environment that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group. Images are hosted in an Amazon S3 bucket using a custom domain name. During a flash sale with 10,000 simultaneous users, some images on the website are not loading. What should be done to resolve the performance issue?

A. Move the images to the EC2 instances in the Auto Scaling group.
B. Enable Transfer Acceleration for the S3 bucket.
C. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
D. Increase the number of minimum, desired, and maximum EC2 instances in the Auto Scaling group.

Commented [LC735]: ANSWER

Question #262

A solutions Architect is designing a new workload where an AWS Lambda function will access an Amazon DynamoDB table. What is the MOST secure means of granting the Lambda function access to the DynamoDB table?

A. Create an identity and access management (IAM) role with the necessary permissions to access the DynamoDB table, and assign the role to the Lambda function.
B. Create a DynamoDB user name and password and give them to the Developer to use in the Lambda function.
C. Create an identity and access management (IAM) user, and create access and secret keys for the user. Give the user the necessary permissions to access the DynamoDB table. Have the Developer use these keys to access the resources.
D. Create an identity and access management (IAM) role allowing access from AWS Lambda and assign the role to the DynamoDB table.

Commented [LC736]: ANSWER

Question #263

A web application runs on Amazon EC2 instances behind an ELB Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones. Every night, the Auto Scaling group doubles in size. traffic analysis shows that users in a particular region are requesting the same static content stored locally on the EC2 instances. How can a Solutions Architect reduce the need to scale and improve application performance for the users?

A. Re-deploy the application in a new VPC that is closer to the users making the requests.
B. Create an Amazon CloudFront distribution for the site and redirect user traffic to the distribution.
C. Store the contents on Amazon EFS instead of the EC2 root volume.
D. Implement Amazon Redshift to create a repository of the content closer to the users.

Commented [LC737]: ANSWER

Question #264

A Solutions Architect is designing an application that will run on Amazon ECS behind an Application Load Balancer (ALB). For security reasons, the Amazon EC2 host instances for the ECS cluster are in a private subnet. What should be done to ensure that the incoming traffic to the host instances is from the ALB only?

A. Create network ACL rules for the private subnet to allow incoming traffic on ports 32768 through 61000 from the IP address of the ALB only.
B. Update the EC2 cluster security group to allow incoming access from the IP address of the ALB only.
C. Modify the security group used by the EC2 cluster to allow incoming traffic from the security group used by the ALB only.
D. Enable AWS WAF on the ALB and enable the ECS rule.

Commented [LC738]: ANSWER

Question #265

A company wants to improve latency by hosting images within a public Amazon S3 bucket fronted by an Amazon CloudFront distribution. The company wants to restrict access to the S3 bucket to include the CloudFront distribution only, while also allowing CloudFront to continue proper functionality. What should be done after making the bucket private to restrict access with the LEAST operational overhead?

A. Create a CloudFront origin access identity and create a security group that allows access from CloudFront.
B. Create a CloudFront origin access identity and update the bucket policy to grant access to it.
C. Create a bucket policy restricting all access to the bucket to include CloudFront IPs only.

Commented [LC739]: ANSWER

D. Enable the CloudFront option to restrict viewer access and update the bucket policy to allow the distribution.

Question #266

A Solutions Architect is designing a new architecture that will use an Amazon EC2 Auto Scaling group. Which of the following factors determine the health check grace period? (Select TWO.)

A. How frequently the Auto Scaling group scales up or down.
B. How many Amazon CloudWatch alarms are Configured for status checks.
C. How much of the application code is embedded in the AMI.
D. How long it takes for the Auto Scaling group to detect a failure.
E. How long the bootstrap script takes to run.

Commented [LC740]: ANSWER

Commented [LC741]: Health grace period is defined as per ref.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/healthcheck.html#health-check-grace-period

Question #267

A company plans to deploy a new application in AWS that reads and writes information to a database. The company wants to deploy the application in two different AWS Regions in an active-active configuration. The databases need to replicate to keep information in sync. What should be used to meet these requirements?

A. Amazon Athena with Amazon S3 cross-region replication.
B. AWS Database Migration Service with change data capture.
C. Amazon DynamoDB with global tables.
D. Amazon RDS for PostgreSQL with a cross-region Read Replica.

Commented [LC742]: ANSWER

Question #268

A company is developing a data lake solution in Amazon S3 to analyse large-scale datasets. The solution makes infrequent SQL queries only. In addition, the company wants to minimize infrastructure costs. Which AWS service should be used to meet these requirements?

A. Amazon Athena.
B. Amazon Redshift Spectrum.
C. Amazon RDS for PostgreSQL.
D. Amazon Aurora.

Commented [LC743]: ANSWER

Question #269

A company needs to store data for 5 years. The company will need to have immediate and highly available access to the data at any point in time, but will not require frequent access. What lifecycle action should be taken to meet the requirements while reducing costs?

A. Transition objects from Amazon S3 Standard to Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
B. Transition objects to expire after 5 years.
C. Transition objects from Amazon S3 Standard to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).
D. Transition objects from Amazon S3 Standard to the GLACIER storage class.

Commented [LC744]: ANSWER

Question #270

A company wants to create an application that will transmit protected health information (PHI) to thousands of service consumers in different AWS accounts. The application servers will sit in private VPC subnets. The routing for the application must be fault tolerant. What should be done to meet these requirements?

A. Create a VPC endpoint service and grant permissions to specific service consumers to create a connection.
B. Create a virtual private gateway connection between each pair of service provider VPCs and service consumer VPCs.
C. Create an internal Application Load Balancer in the service provider VPC and put application servers behind it.
D. Create a proxy server in the service provider VPC to route requests from service consumers to the application servers.

Commented [LC745]: https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints.html

Question #271

A company hosts a website using Amazon API Gateway on the front end. Recently, there has been heavy traffic on the website and the company wants to control access by allowing authenticated traffic only. How should the company limit access to authenticated users only? (Select TWO.)

A. Allow users that are authenticated through Amazon Cognito.
B. Limit traffic through API Gateway.
C. Allow X.509 certificates to authenticate traffic.
D. Deploy AWS KMS to identify users.
E. Assign permissions in AWS IAM to allow users.

Commented [LC746]: ANSWER

Commented [LC747]: ANSWER

Question #272

A company needs to use AWS resources to expand capacity for a website hosted in an on-premises data center. The AWS resources will include load balancers, Auto Scaling, and Amazon EC2 instances that will access an on-premises database. Network connectivity has been established, but no traffic is going to the AWS environment. How should Amazon Route 53 be Configured to distribute load to the AWS environment? (Select TWO.)

A. Set up a weighted routing policy, distributing the workload between the load balancer and the on-premises environment.
B. Set up an A record to point the DNS name to the IP address of the load balancer.
C. Create multiple A records for the EC2 instances.
D. Set up a geolocation routing policy to distribute the workload between the load balancer and the on-premises environment.
E. Set up a routing policy for failover using the on-premises environment as primary and the load balancer as secondary.

Commented [LC748]: ANSWER

Commented [LC749]: ANSWER

Question #273

Users submit requests to a service that takes several minutes to process. A Solutions Architect needs to ensure that these requests are processed at least once, and that the service has the ability to handle large increases in the number of requests. How should these requirements be met?

A. Put the requests into an Amazon SQS queue and Configure Amazon EC2 instances to poll the queue.
B. Publish the message to an Amazon SNS topic that an Amazon EC2 subscriber can receive and process.
C. Save the requests to an Amazon DynamoDB table with a DynamoDB stream that triggers an Amazon EC2 Spot Instance.
D. Use Amazon S3 to store the requests and Configure an event notification to have Amazon EC2 instances process the new object.

Commented [LC750]: ANSWER

Question #274

A Solutions Architect is designing an Amazon VPC that requires access to a remote API server using IPv6. Resources within the VPC should not be accessed directly from the Internet. How should this be achieved?

A. Use a NAT gateway and deny public access using security groups.
B. Attach an egress-only internet gateway and update the routing tables.
C. Use a NAT gateway and update the routing tables.
D. Attach an internet gateway and deny public access using security groups.

Commented [LC751]: ANSWER

Question #275

When designing an Amazon SQS message-processing solution, messages in the queue must be processed before the maximum retention time has elapsed. Which actions will meet this requirement? (Choose two.)

A. Use AWS STS to process the messages.
B. Use Amazon EBS-optimized Amazon EC2 instances to process the messages.
C. Use Amazon EC2 instances in an Auto Scaling group with scaling triggered based on the queue length.
D. Increase the SQS queue attribute for the message retention period.
E. Convert the SQS queue to a first-in-first-out (FIFO) queue.

Commented [LC752]: To speed up the processing

Commented [LC753]: To parallelize the processing

Question #276

A company deployed a three-tier web application on Amazon EBS backed Amazon EC2 instances for the web and application tiers, and Amazon RDS for the database tier. The company is concerned about loss of data in the web and application tiers. What is the MOST efficient way to prevent data loss?

A. Create an Amazon EFS file system and run a shell script to copy the data.
B. Create an Amazon EBS snapshot using an Amazon CloudWatch Events rule.
C. Create an Amazon S3 snapshot policy to back up the Amazon EBS volumes.
D. Create a snapshot lifecycle policy that takes periodic snapshots of the Amazon EBS volumes.

Commented [LC754]: ANSWER

Question #277

A company is using Amazon S3 for backups from an on-premises environment. Regulatory requirements state that data must be retained for at least 7 years. The data is infrequently accessed for 35 days, but needs to be instantly available. After 35 days, the data is rarely accessed. Which combination of actions will provide the MOST cost-effective solution? (Choose two)

A. Change the backup so the data goes to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) directly.
B. Create an S3 lifecycle policy that moves the data to the GLACIER storage class after 7 years.
C. Change the backup so the data goes to Amazon Glacier directly.
D. Create an S3 lifecycle policy that moves the data to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 35 days.
E. Creates an S3 lifecycle policy that moves the data to the GLACIER storage class after 35 days.

Commented [LC755]: ANSWER

Commented [LC756]: ANSWER

Question #278

A Solutions Architect is building an online shopping application where users will be able to browse items, add items to a cart, and purchase the items. Images of items will be stored in Amazon S3 buckets organized by item category. When an item is no longer available for purchase, the item image will be deleted from the S3 bucket. Occasionally, during testing, item images deleted from the S3 bucket are still visible to some users. What is a flaw in this design approach?

A. Defining S3 buckets by item may cause partition distribution errors, which will impact performance.
B. Amazon S3 DELETE requests are eventually consistent, which may cause other users to view items that have already been purchased.
C. Amazon S3 DELETE requests apply a lock to the S3 bucket during the operation, causing other users to be blocked.
D. Using Amazon S3 for persistence exposes the application to a single point of failure.

Commented [LC757]: ANSWER

Question #279

A Solution Architect is creating a serverless web application that must access mapping data in hundreds of data files, each containing approximately 30 KB of data. The storage required is expected to grow to hundreds of terabytes. Which storage solution is most cost-effective, yet still meets the requirements for this use case?

A. Amazon EFS.
B. Amazon EBS Cold HDD (sc1).
C. Amazon S3 Standard.
D. Amazon DynamoDB.

Commented [LC758]: ANSWER

Question #280

An application running on AWS Lambda requires an API key to access a third-party service. The key must be stored securely with audited access to the Lambda function only. What is the MOST secure way to store the key?

A. As an object in Amazon S3.
B. As a secure string in AWS Systems Manager Parameter Store.
C. Inside a file on an Amazon EBS volume attached to the Lambda function.
D. Inside a secrets file stored on Amazon EFS.

Commented [LC759]: ANSWER

Question #281

An application produces monthly reports that must be immediately accessible for up to 7 days. After 7 days, the data can be archived. Compliance policies require that the archived data be retrievable within 24 hours of a request. What is the MOST cost-effective approach to satisfy the compliance requirement?

A. Store the data in Amazon S3 Standard storage with a lifecycle rule to transition the data to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days, then transition to the GLACIER storage class after 30 days.
B. Store the data in Amazon S3 Standard storage with a lifecycle rule to transition the data to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.
C. Store the data in Amazon S3 Standard storage with a lifecycle rule to transition the data to the GLACIER storage class after 30 days.
D. Store the data in Amazon S3 Standard storage with a lifecycle rule to transition the data to the GLACIER storage class after 7 days.

Commented [LC760]: ANSWER

Question #282

A company is developing a new stateless web service with low memory requirements. The service needs to scale based on demand. What is the MOST cost-effective solution?

A. Deploy the application onto AWS Elastic Beanstalk.
B. Deploy the application onto AWS Lambda with access through Amazon API Gateway.
C. Deploy the application onto an Amazon EC2 Spot Fleet.
D. Deploy the application onto a container with an Amazon ECS EC2 launch type.

Commented [LC761]: ANSWER

Question #283

A company has an application that generates invoices and makes the invoices available online. Invoices are stored as PDFs in an Amazon S3 bucket. Customers typically only view each invoice during the month it is issued. However, past invoices need to be immediately available. There are concerns over rising storage costs as the company gains more customers. What is the MOST cost-effective method to store the data?

A. Use Amazon S3 for current invoices. Set up lifecycle rules to migrate invoices to the GLACIER storage class after 30 days.
B. Store the invoices as text files. Use Amazon CloudFront to convert the invoices from text to PDF when customers download invoices.
C. Store the invoices as binaries in an Amazon RDS database instance. Retrieve them from the database when customers request invoices.

D. Use Amazon S3 for current invoices. Set up lifecycle rules to migrate invoices to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

Commented [LC762]: ANSWER

Question #284

A company is running its application in a single region on Amazon EC2 with Amazon EBS and Amazon S3 part of the storage design. What should be done to reduce data transfer costs?

A. Create a copy of the compute environment in another region.
B. Convert the application to run on Lambda@Edge.
C. Create an Amazon CloudFront distribution with Amazon S3 as the origin.
D. Replicate Amazon S3 data to buckets in regions closer to the requester.

Commented [LC763]: ANSWER

Question #285

An application server needs to be in a private subnet without access to the Internet. The solution must retrieve and upload files to an Amazon S3 bucket. How should a Solutions Architect design a solution to meet these requirements?

A. Use Amazon S3 VPC endpoints.
B. Deploy a proxy server.
C. Use a NAT Gateway.
D. Use a private Amazon S3 bucket.

Commented [LC764]: ANSWER

Question #286

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access. Which of the following would be the LEAST complicated implementation?

A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
B. Use an S3 bucket and provide direct access to the le. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URl.
D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL, and recreate the URL as necessary.

Commented [LC765]: ANSWER

Question #287

A Solutions Architect plans to migrate a load balancer tier from a data center to AWS. Several websites have multiple domains that require secure load balancing. The Architect decides to use Elastic Load Balancing Application Load Balancers. What is the MOST efficient method for achieving secure communication?

A. Create a wildcard certificate and upload it to the Application Load Balancer.
B. Create an SNI certificate and upload it to the Application Load Balancer.
C. Create a secondary proxy server to terminate SSL traffic before the traffic reaches the Application Load Balancer.
D. Let a third-party certificate Manager manage certificates required to all domains and upload them to the Application Load Balancer.

Commented [LC766]: ANSWER

Question #288

An application stores data in an Amazon RDS MySQL DB instance. The database traffic primarily consists of read queries, which are overwhelming the current database. A Solutions Architect wants to scale the database. What combination of steps will achieve the goal? (Choose two.)

A. Add the MySQL database instances to an Auto Scaling group.
B. Migrate the MySQL database to Amazon Aurora.
C. Migrate the MySQL database to a PostgreSQL database.
D. Create read replicas in different Availability Zones.
E. Create an ELB Application Load Balancer.

Commented [LC767]: ANSWER

Commented [LC768]: ANSWER

Question #289

A Solutions Architect is designing an elastic application that will have between 10 and 50 Amazon EC2 concurrent instances running, dependent on load. Each instance must mount storage that will read and write to the same 50 GB folder. Which storage type meets the requirements?

A. Amazon S3.

B. Amazon EFS.
C. Amazon EBS volumes.
D. Amazon EC2 instance store.

Commented [LC769]: ANSWER

Question #290

A Solutions Architect is designing an application that is expected to have millions of users. The Architect needs options to store session data. Which option is the MOST performant?

A. Amazon ElastiCache.
B. Amazon RDS.
C. Amazon S3.
D. Amazon EFS.

Commented [LC770]: ANSWER

Question #291

A company is launching a dynamic website, and the Operations team expects up to 10 times the traffic on the launch date. This website is hosted on Amazon EC2 instances and traffic is distributed by Amazon Route 53. A Solutions Architect must ensure that there is enough backend capacity to meet user demands. The Operations team wants to scale down as quickly as possible after the launch. What is the MOST cost-effective and fault-tolerant solution that will meet the company's customer demands? (Choose two.)

A. Set up an Application Load Balancer to distribute traffic to multiple EC2 instances.
B. Set up an Auto Scaling group across multiple Availability Zones for the website, and create scale-out and scale-in policies.
C. Create an Amazon CloudWatch alarm to send an email through Amazon SNS when EC2 instances experience higher loads.
D. Create an AWS Lambda function to monitor website load time, run it every 5 minutes, and use the AWS SDK to create a new instance if website load time is longer than 2 seconds.
E. Use Amazon CloudFront to cache the website content during launch and set a TTL for cache content to expire after the launch date.

Commented [LC771]: ANSWER

Commented [LC772]: ANSWER

Question #292

A customer has an application that is used by enterprise customers outside of AWS. Some of these customers use legacy firewalls that cannot whitelist by DNS name, but whitelist based only on IP address. The application is currently deployed in two Availability Zones, with one EC2 instance in each that has Elastic IP addresses. The customer wants to whitelist only two IP addresses, but the two existing EC2 instances cannot sustain the amount of traffic. What can a Solutions Architect do to support the customer and allow for more capacity? (Choose two.)

A. Create a Network Load Balancer with an interface in each subnet, and assign a static IP address to each subnet.
B. Create additional EC2 instances and put them on standby. Remap an Elastic IP address to a standby instance in the event of a failure.
C. Use Amazon Route 53 with a weighted, round-robin routing policy across the Elastic IP addresses to resolve one at a time.
D. Add additional EC2 instances with Elastic IP addresses, and register them with Amazon Route 53.
E. Switch the two existing EC2 instances for an Auto Scaling group, and register them with the Network Load Balancer.

Commented [LC773]: ANSWER

Commented [LC774]: ANSWER

Question #293

A company is storing application data in Amazon S3 buckets across multiple AWS regions. Company policy requires that encryption keys be generated at the company headquarters, but the encryption keys may be stored in AWS after generation. The Solutions Architect plans to Configure cross-region replication. Which solution will encrypt the data whole requiring the LEAST amount of operational overhead?

A. Configure the applications to write to an S3 bucket using client-side encryption.
B. Configure S3 buckets to encrypt using AES-256.
C. Configure S3 object encryption using AWS CLI with Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).
D. Configure S3 buckets to use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) with imported key material in both regions.

Commented [LC775]: ANSWER

Question #294

A Solutions Architect must design a solution that encrypts data in Amazon S3. Corporate policy mandates encryption keys be generated and managed on premises. Which solution should the Architect use to meet the security requirements?

A. AWS CloudHSM.
B. SSE-KMS: Server-side encryption with AWS KMS managed keys.
C. SSE-S3: Server-side encryption with Amazon-managed master key.
D. SSE-C: Server-side encryption with customer-provided encryption keys.

Commented [LC776]: ANSWER

Question #295

A Solutions Architect is considering possible options for improving the security of the data on an Amazon EBS volume attached to an Amazon EC2 instance. Which solution will improve the security of the data?

A. Use AWS KMS to encrypt the EBS volume.
B. Create an IAM policy that restricts read and write access to the volume.
C. Migrate the sensitive data to an instance store volume.
D. Use Amazon single sign-on to control login access to the EC2 instance.

Commented [LC777]: ANSWER

Question #296

A Solutions Architect designed a system based on Amazon Kinesis Data Streams. After the workflow was put into production, the company noticed it performed slowly and identified Kinesis Data Streams as the problem. One of the streams has a total of 10 Mb/s throughput. What should the Solutions Architect recommend to improve performance?

A. Use AWS Lambda to preprocess the data and transform the records into a simpler format, such as CSV.
B. Run the MergeShard command to reduce the number of shards that the consumer can more easily process.
C. Change the workflow to use Amazon Kinesis Data Firehose to gain a higher throughput.
D. Run the UpdateShardCount command to increase the number of shards in the stream.

Commented [LC778]: ANSWER

Question #297

A Solutions Architect is designing an application that requires having six Amazon EC2 instances running at all times. The application will be deployed in the sa-east-1 region, which has three Availability Zones: sa-east-1a, sa-east-1b, and sa-east-1c. Which action will provide 100 percent fault tolerance and the LOWEST cost in the event that one Availability Zone in the region becomes unavailable?

A. Deploy six Amazon EC2 instances in sa-east-1a, six Amazon EC2 instances in sa-east-1b, and six Amazon EC2 instances in sa-east-1c.
B. Deploy six Amazon EC2 instances in sa-east-1a, four Amazon EC2 instances in sa-east-1b, and two Amazon EC2 instances in sa-east-1c.
C. Deploy three Amazon EC2 instances in sa-east-1a, three Amazon EC2 instances in sa-east-1b, and three Amazon EC2 instances in sa-east-1c.
D. Deploy two Amazon EC2 instances in sa-east-1a, two Amazon EC2 instances in sa-east-1b, and two Amazon EC2 instances in sa-east-1c.

Commented [LC779]: ANSWER

Question #298

A Solutions Architect is designing a three-tier web application that will allow customers to upload pictures from a mobile application. The application will then generate a thumbnail of the picture and return a message to the user confirming that the image was successfully uploaded. Generation of the thumbnail may take up to 5 seconds. To provide a sub second response time to the customers uploading the images, the Solutions Architect wants to separate the web tier from the application tier. Which service would allow the presentation tier to asynchronously dispatch the request to the application tier?

A. AWS Step Functions.
B. AWS Lambda.
C. Amazon SNS.
D. Amazon SQS.

Commented [LC780]: ANSWER

Question #299

A Solutions Architect is designing an application in AWS. The Architect must not expose the application or database tier over the Internet for security reasons. The application must be low-cost and have a scalable front end. The databases and application tier must have only one-way Internet access to download software and patch updates. Which solution helps to meet these requirements?

A. Use a NAT Gateway as the front end for the application tier and to enable the private resources to have Internet access.
B. Use an Amazon EC2-based proxy server as the front end for the application tier, and a NAT Gateway to allow Internet access for private resources.
C. Use an ELB Classic Load Balancer as the front end for the application tier, and an Amazon EC2 proxy server to allow Internet access for private resources.
D. Use an ELB Classic Load Balancer as the front end for the application tier, and a NAT Gateway to allow Internet access for private resources.

Commented [LC781]: ANSWER

Questions 300-312

Question #300

A Solutions Architect is designing a multi-tier application consisting of an Application Load Balancer, an Amazon RDS database instance, and an Auto Scaling group on Amazon EC2 instances. Each tier is in a separate subnet. There are some EC2 instances in the subnet that belong to another application. The RDS database instance should accept traffic only from the EC2 instances in the Auto Scaling group. What should be done to meet these requirements?

A. Configure the inbound network ACLs on the database subnet to accept traffic from the IP addresses of the EC2 instances only.
B. Configure the inbound rules on the security group associated with the RDS database instance. Set the source to the security group associated with instances in the Auto Scaling group.
C. Configure the outbound rules on the security group associated with the Auto Scaling group. Set the destination to the security group associated with the RDS database instance.
D. Configure the inbound network ACLs on the database subnet to accept traffic only from the CIDR range of the subnet used by the Auto Scaling group.

Commented [LC782]: ANSWER

Question #301

An organization uses Amazon S3 to store video content served via its website. It only has rights to deliver this content to users within its own country and needs to restrict access. How can the organization ensure that these files are only accessible from within its country?

A. Use a custom Amazon S3 bucket policy to allow access only to users inside the organization's country.
B. Use Amazon CloudFront and Geo Restriction to allow access only to users inside the organization's country.
C. Use an Amazon S3 bucket ACL to allow access only to users inside the organization's country.
D. Use file-based ACL permissions on each video file to allow access only to users inside the organization's country.

Commented [LC783]: ANSWER

Question #302

A company is storing data in an Amazon DynamoDB table and needs to take daily backups and retain them for 6 months. How should the Solutions Architect meet these requirements without impacting the production workload?

A. Use DynamoDB replication and restore the table from the replica.
B. Use AWS Data Pipeline and create a scheduled job to back up the DynamoDB table daily.
C. Use Amazon CloudWatch Events to trigger an AWS Lambda function that makes an on-demand backup of the table.
D. Use AWS Batch to create a scheduled backup with the default template, then back up to Amazon S3 daily.

Commented [LC784]: A is too manual job. B is not possible because it transforms and elaborates on various sources, so it's for a different purpose. D as well.

C makes sense.

Question #303

A client reports that they want see an audit log of any changes made to AWS resources in their account. What can the client do to achieve this?

A. Set up Amazon CloudWatch monitors on services they own.
B. Enable AWS CloudTrail logs to be delivered to an Amazon S3 bucket.
C. Use Amazon CloudWatch Events to parse logs.
D. Use AWS OpsWorks to manage their resources.

Commented [LC785]: ANSWER

Question #304

An application running in a private subnet accesses an Amazon DynamoDB table. There is a security requirement that the data never leave the AWS network. How should this requirement be met?

A. Configure a network ACL on DynamoDB to limit traffic to the private subnet.
B. Enable DynamoDB encryption at rest using an AWS KMS key.
C. Add a NAT gateway and Configure the route table on the private subnet.
D. Create a VPC endpoint for DynamoDB and Configure the endpoint policy.

Commented [LC786]: ANSWER

Question #305

A three-tier application is being created to host small news articles. The application is expected to serve millions of users. When breaking news occurs, the site must handle very large spikes in traffic without significantly impacting database performance. Which design meets these requirements while minimizing costs?

A. Use Auto Scaling groups to increase the number of Amazon EC2 instances delivering the web application.
B. Use Auto Scaling groups to increase the size of the Amazon RDS instances delivering the database.
C. Use Amazon DynamoDB strongly consistent reads to adjust for the increase in traffic.
D. Use Amazon DynamoDB Accelerator (DAX) to cache read operations to the database.

Commented [LC787]: This question is missing a key concept which is the underlying DB. Poorly written question, my suggestion is D. A doesn't help the web app in any case. B scales vertically which is something not relatable to our situation. C is wrong for obvious reasons, going strongly consistent makes the performance worse than they are, that is the reason eventual consistency has been developed for.

Question #306

During a review of business applications, a Solutions Architect identifies a critical application with a relational database that was built by a business user and is running on the user's desktop. To reduce the risk of a business interruption, the Solutions Architect wants to migrate the application to a highly available, multi-tiered solution in AWS. What should the Solutions Architect do to accomplish this with the LEAST amount of disruption to the business?

A. Create an import package of the application code for upload to AWS Lambda, and include a function to create another Lambda function to migrate data into an Amazon RDS database.
B. Create an image of the user's desktop, migrate it to Amazon EC2 using VM Import, and place the EC2 instance in an Auto Scaling group.
C. Pre-stage new Amazon EC2 instances running the application code on AWS behind an Application Load Balancer and an Amazon RDS MultiAZ DB instance.
D. Use AWS DMS to migrate the backend database to an Amazon RDS Multi-AZ DB instance. Migrate the application code to AWS Elastic Beanstalk.

Commented [LC788]: ANSWER

Question #307

A company has thousands of files stored in an Amazon S3 bucket that has a well-defined access pattern. The files are accessed by an application multiple times a day for the rest 30 days. Files are rarely accessed within the next 90 days. After that, the files are never accessed again. During the rest 120 days accessing these files should never take more than a few seconds. Which lifecycle policy should be used for the S3 objects to minimize costs based on the access pattern?

A. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage for the rest 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.
B. Use Amazon S3 Standard storage for the rest 30 days. Then move the files to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the next 90 days. Allow the data to expire after that.
C. Use Amazon S3 Standard storage for rest 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.
D. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the rest 30 days. After that, move the data to the GLACIER storage class, where is will be deleted automatically.

Commented [LC789]: ANSWER

Question #308

A company creates business-critical 3D images every night. The images are batch-processed every Friday and require an uninterrupted 48 hours to complete. What is the MOST cost-effective Amazon EC2 pricing model for this scenario?

A. On-Demand Instances.
B. Scheduled Reserved Instances.
C. Reserved Instances.
D. Spot Instances.

Commented [LC790]: ANSWER

Question #309

An application generates audit logs of operational activities. Compliance requirements mandate that the application retain the logs for 5 years. How can these requirements be met?

A. Save the logs in an Amazon S3 bucket and enable Multi-Factor Authentication Delete (MFA Delete) on the bucket.
B. Save the logs in an Amazon EFS volume and use Network File System version 4 (NFSv4) locking with the volume.
C. Save the logs in an Amazon Glacier vault and use the Vault Lock feature.
D. Save the logs in an Amazon EBS volume and take monthly snapshots.

Commented [LC791]: ANSWER

Question #310

A Solutions Architect is creating an application running in an Amazon VPC that needs to access AWS Systems Manager Parameter Store. Network security rules prohibit any route table entry with a 0.0.0.0/0 destination. What infrastructure addition will allow access to the AWS service while meeting the requirements?

A. VPC peering.
B. NAT instance.
C. NAT gateway.
D. AWS PrivateLink.

Commented [LC792]: ANSWER

Question #311

A photo-sharing website running on AWS allows users to generate thumbnail images of photos stored in Amazon S3. An Amazon DynamoDB table maintains the locations of photos, and thumbnails are easily re-created from the originals if they are accidentally deleted. How should the thumbnail images be stored to ensure the LOWEST cost?

A. Amazon S3 Standard-Infrequent Access (S3 Standard-IA) with cross-region replication.
B. Amazon S3.
C. Amazon Glacier.
D. Amazon S3 with cross-region replication.

Commented [LC793]: ANSWER

Question #312

A company is implementing a data lake solution on Amazon S3. Its security policy mandates that the data stored in Amazon S3 should be encrypted at rest. Which options can achieve this? (Select TWO.)

A. Use S3 server-side encryption with an Amazon EC2 key pair.
B. Use S3 server-side encryption with customer-provided keys (SSE-C).
C. Use S3 bucket policies to restrict access to the data at rest.
D. Use client-side encryption before ingesting the data to Amazon S3 using encryption keys.
E. Use SSL to encrypt the data while in transit to Amazon S3.

Commented [LC794]: ANSWER

Commented [LC795]: ANSWER

Uncatalogued Questions

Question #1

A reporting application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones. Due to their complexity, some reports may take up to 15 minutes to respond to a request. A solutions architect is concerned that users will receive 500 errors if a report request is in process during a scale-in event. Which action will ensure that user requests are completed before instances are terminated?

A. Enable sticky sessions for the target group of the instances.
B. Enable connection draining on the Application Load Balancer.
C. Increase the cooldown period for the Auto Scaling group to greater than 1,500 seconds.
D. Increase the deregistration delay timeout for the target group of the instances to greater than 1,500 seconds.

Question #2

A company is deploying an application that processes large quantities of data in batches as needed. The company plans to use Amazon EC2 instances for the workload. The network architecture must support a highly scalable solution and prevent groups of nodes from sharing the same underlying hardware. Which combination of network solutions will meet these requirements? (Select TWO.)

A. Create Capacity Reservations for the EC2 instances to run in a placement group.
B. Run the EC2 instances in a spread placement group.
C. Run the EC2 instances in a cluster placement group.
D. Place the EC2 instances in an EC2 Auto Scaling group.
E. Run the EC2 instances in a partition placement group.

Question #3

A company has 2 VPCs named Management and Production. The Mgt VPC uses VPNs through customer gateway to connect to a single device in the data center. The Prod VPC uses VPG with two attached AWS direct connect connections. The Mgt and Prod VPCs both use a single VPC steering connection to allow communication between applications. What should a solution architect do to mitigate any single point of failure in this architecture?

A. Add a set of VPNs between Mgt and Prod VPCs.
B. Add a second virtual private gateway and attach it to Mgt VPC.
C. Add a second set of VPNs to Mgt VPC from second customer gateway device.
D. Add a second VPC peering connection between the Mgt VPC and Prod VPC.

Question #4

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets. Which steps should a solutions architect take to block requests from unauthorized users? (Choose two.)

A. Create a usage plan with an API key that is shared with genuine users only.
B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.
C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.
D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.
E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

Question #5

A company has migrated a two-tier application from its on-premises data center to the AWS Cloud. The data tier is a Multi-AZ deployment of Amazon RDS for Oracle with 12 TB of General Purpose SSD Amazon Elastic Block Store (Amazon EBS) storage. The application is designed to process and store documents in the database as binary large objects (blobs) with an average document size of 6 MB. The database size has grown over time, reducing the performance and increasing the cost of storage. The company must improve the database performance and needs a solution that is highly available and resilient. Which solution will meet these requirements MOST cost-effectively?

A. Reduce the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Magnetic.
B. Increase the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Provisioned IOPS.
C. Create an Amazon S3 bucket. Update the application to store documents in the S3 bucket. Store the object metadata in the existing database.
D. Create an Amazon DynamoDB table. Update the application to use DynamoDB. Use AWS Database Migration Service (AWS DMS) to migrate data from the Oracle database to DynamoDB.

Missing Questions Set #1

1		51		101		151	M	201	M	251		301		351		401		451		501	
2		52		102		152	M	202	M	252		302		352		402		452		502	
3		53		103		153	M	203	M	253		303		353		403		453		503	
4		54		104		154	M	204	M	254		304		354		404		454		504	
5		55		105		155	M	205	M	255		305		355		405		455		505	
6		56		106		156	M	206	M	256		306		356		406		456		506	
7		57		107		157	M	207	M	257		307		357		407		457		507	
8		58		108		158	M	208	M	258		308		358		408		458		508	
9		59		109		159	M	209	M	259		309		359		409		459		509	
10		60		110		160	M	210	M	260		310		360		410		460		510	
11		61		111		161	M	211		261		311		361		411		461		511	
12		62		112		162	M	212		262		312		362		412		462		512	
13		63		113		163	M	213		263		313		363		413		463		513	
14		64		114		164	M	214		264		314		364		414		464		514	
15		65		115		165	M	215		265		315		365		415		465		515	
16		66		116		166	M	216		266		316		366		416		466		516	
17		67		117		167	M	217		267		317		367		417		467		517	
18		68		118		168	M	218		268		318		368		418		468		518	
19		69		119		169	M	219		269		319		369		419		469		519	
20		70		120		170	M	220		270		320		370		420		470		520	
21		71		121		171	M	221		271		321		371		421		471		521	
22		72		122		172	M	222		272		322		372		422		472		522	
23		73		123		173	M	223		273		323		373		423		473		523	
24		74		124		174	M	224		274		324		374		424		474		524	
25		75		125		175	M	225		275		325		375		425		475		525	
26		76		126		176	M	226		276		326		376		426		476		526	
27		77		127		177	M	227		277		327		377		427		477		527	
28		78		128		178	M	228		278		328		378		428		478		528	
29		79		129		179	M	229		279		329		379		429		479		529	
30		80		130		180	M	230		280		330		380		430		480		530	
31		81		131		181	M	231		281		331		381		431		481	M	531	
32		82		132		182	M	232		282		332		382		432		482		532	
33		83		133		183	M	233		283		333		383		433		483		533	
34		84		134		184	M	234		284		334		384		434		484		534	
35		85		135		185	M	235		285		335		385		435		485		535	
36		86		136		186	M	236		286		336		386		436		486		536	
37		87		137		187	M	237		287		337		387		437		487		537	
38		88		138		188	M	238		288		338		388		438		488		538	
39		89		139		189	M	239		289		339		389		439		489		539	
40		90		140		190	M	240		290		340		390		440		490		540	
41		91		141	M	191	M	241		291		341		391		441		491		541	
42		92		142	M	192	M	242		292		342		392		442		492		542	
43		93		143	M	193	M	243		293		343		393		443		493		543	
44		94		144	M	194	M	244		294		344		394		444		494		544	
45		95		145	M	195	M	245		295		345		395		445		495		545	
46		96		146	M	196	M	246		296		346		396		446		496		546	
47		97		147	M	197	M	247		297		347		397		447		497		547	
48		98		148	M	198	M	248		298		348		398		448		498		548	
49		99		149	M	199	M	249		299		349		399		449		499		549	
50		100		150	M	200	M	250		300		350		400		450		500		550	