Exam : **AWS-Solutions-Associate**

Title : AWS Certified Solutions Architect - Associate

Vendor : Amazon

Version : V19.75

NO.1 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 workflow?
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.
Answer: C
Explanation
https://aws.amazon.com/about-aws/whats-new/2019/11/amazon-sns-adds-support-for-dead-letter-queues-dlq/
https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html

NO.2 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.
Answer: D

NO.3 An application runs in a VPC on Amazon EC2 instances behind an Application Load Balancer. Traffic to the Amazon EC2 instances must be limited to traffic from the Application Load Balancer.
Based on these requirements, the security group configuration should only allow traffic from:
A. the public IPs of the Application Load Balancer nodes.
B. the IP range of the Application Load Balancer subnets.
C. the security group attached to the Application Load Balancer.
D. the VPC CIDR.
Answer: C

NO.4 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.

Answer: B

NO.5 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
Answer: C

NO.6 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
Answer: D
Explanation
https://docs.aws.amazon.com/AmazonS3/latest/dev/replication-config-for-kms-objects.html#replication-kms-ext

NO.7 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
Answer: B

NO.8 An organization hosts 10 microservices, each in an Auto Scaling group behind individual Classic Load Balancers. Each EC2 instance is running at optimal load. Which of the following actions would allow the organization to reduce costs without impacting performance?
A. Reduce the number of EC2 instances behind each Classic Load Balancer
B. Change instance types in the Auto Scaling group launch configuration

C. Change the maximum size but leave the desired capacity of the Auto Scaling groups
D. Replace the Classic Load Balancers with a single Application Load Balancer
Answer: D
Explanation
https://www.sumologic.com/insight/aws-elastic-load-balancers-classic-vs-application/
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-target-ecs-containers.html An application load balancer can take the place of multiple individual classic load balancers to load balance microservices (e.g. running on AWS ECS) saving costs.

NO.9 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
Answer: D

NO.10 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 fix 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.
Answer: B
Explanation
https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application. To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. The scheduled action tells Amazon EC2 Auto Scaling to perform a scaling action at specified times. To create a scheduled scaling action, you specify the start time when the scaling action should take effect, and the new minimum, maximum, and desired sizes for the scaling action. At the specified time, Amazon EC2 Auto Scaling updates the group with the values for minimum, maximum, and desired size specified by the scaling action. You

can create scheduled actions for scaling one time only or for scaling on a recurring schedule.

NO.11 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

Answer: A

NO.12 A Solutions Architect is designing a feature for internal-facing employees of a call center that permits users to toggle their availability to take a call. This feature should be available through a link found in the call center support application. When a user signals their availability, the call center manager receives an SMS and a status board should update with the user's availability.
Which combination of AWS services can satisfy this need?

A. Amazon EC2, Amazon DynamoDB, Amazon SQS, Amazon API Gateway, and Amazon S3

B. Lambda, API gateway, DynamoDB, Amazon SNS, and Amazon S3

C. Lambda, Amazon SQS, DynamoDB, API Gateway, and Amazon S3

D. Amazon EC2, API Gateway, AWS Elastic Beanstalk, DynamoDB, and Amazon S3

Answer: B

NO.13 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.

Answer: D

Explanation
When creating load balancers in a VPC, we recommend that you add one subnet per Availability Zone for at least two Availability Zones. This improves the availability of your load balancer. Note that you can modify the subnets for your load balancer at any time.

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-manage-subnets.html

NO.14 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.

Answer: C

NO.15 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.

Answer: C
Explanation
https://linuxacademy.com/blog/linux-academy/scheduling-amazon-dynamodb-backups-with-lambda-python-and

NO.16 A Solutions Architect is designing an API that will use Amazon API Gateway, which is backed by AWS Lambda. The Lambda function is not running inside a VPC and will query Amazon DunamoDB to get the results. The user will include the ItemId request parameter in the URL query string as the key to retrieve the data. The Solutions Architect analysed the traffic patter and has noticed that customers are sending repeated queries to get the same information. The Solution Architect wants to implement a caching to reduce the load on the database and improve query latency.
What should the Solution Architect do to implement a caching solution?

A. in API Gateway, add an additional Cute-Control: only-if -cached header before sending the request to Lambda

B. In API Gateway, enable caching based on the item id query parameter

C. In Lambda, use/tmp as the cache directory to store previously retrieved requests

D. In Amazon ElastiCache. store previously retrieved requests and query the cluster before querying the database.

Answer: B

NO.17 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.
Answer: B

NO.18 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
Answer: C
Explanation
Enabling ElastiCache Multi-AZ with automatic failover on your Redis cluster (in the API and CLI, replication group) improves your fault tolerance. This is true particularly in cases where your cluster's read/write primary cluster becomes unreachable or fails for any reason. Multi-AZ with automatic failover is only supported on Redis clusters that support replication.

NO.19 A legacy build management application stores artifacts in an NFS shared filesystem accessed by 400 servers.
The company is migrating its infrastructure to AWS.
Which storage service should be used for build management?
A. Amazon S3
B. Amazon EFS
C. Amazon EBS
D. Amazon EC2 Instance Storage
Answer: B

NO.20 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.
Answer: C
Explanation
https://docs.amazonaws.cn/en_us/lambda/latest/dg/env_variables.html

NO.21 A company is using Amazon DynamoDB to stage its product catalog, which is 1 GB. Since a product entry, on average, consists of 100 KB of data, and the average traffic is about 250 requests per second, the database administrator has provisioned 3,000 RCU of read capacity throughput. However, some products are very popular and users are experiencing delays or timeouts due to throttling.
What improvement offers a long-term solution to this problem?
A. Increase the throughput provisioning to 6.000 RCUs
B. Use Amazon DynamoDB Accelerator to maintain the frequently read items
C. Augment Amazon DynamoDB by storing only the key product attributes, with the details stored on Amazon S3.
D. Change the partition key to consist of a hash of product key and product type, instead of just the product key.
Answer: B

NO.22 A company is developing a data lake solution in Amazon S3 to analyze 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
Answer: A
Explanation
https://docs.aws.amazon.com/whitepapers/latest/building-data-lakes/in-place-querying.html
Athena is a serverless service and does not need any infrastructure to create, manage, or scale data sets. It works directly on top of Amazon S3 data sets. It creates external tables and therefore does not manipulate S3 data sources.
"You would typically use Athena for ad hoc data discovery and SQL querying, and then use Redshift Spectrum for more complex queries and scenarios where a large number of data lake users want to run concurrent BI and reporting workloads."

NO.23 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.
Answer: B
Explanation

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-autoscaling-triggers.html

NO.24 A company's Data Analysis team needs to perform real-time complex queries against a database. As the team grows, the complex queries are slowing down production transactions. The current environment has an Amazon RDS database with the largest instance type and is still experiencing performance issues.
Which solution will reduce costs and resolve the performance issues?
A. Implement an Amazon RDS Read Replica of the production database to be used by the Data Analysis team and reduce the RDS database instance size.
B. Implement Amazon ElastiCache and run the query against ElastiCache directly.
C. Implement Amazon EC2 instances to run a cluster of the production database and remove the RDS database instance.
D. Implement a larger Amazon RDS database instance type and apply Reserved Instances by submitting a limit increase request.
Answer: A

NO.25 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
Answer: C

NO.26 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 presigned URLs to users.
Answer: C
Explanation
The following example generates a pre-signed URL that enables you to temporarily share a file without making it public. Anyone with access to the URL can view the file.
https://docs.aws.amazon.com/sdk-for-go/v1/developer-guide/s3-example-presigned-urls.html

NO.27 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
Answer: A

NO.28 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
Answer: C

NO.29 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
Answer: C
Explanation
https://aws.amazon.com/about-aws/whats-new/2018/07/amazon-dynamodb-global-tables-regional-expansion/
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.CrossRegionRepl.html
https://aws.amazon.com/es/blogs/database/how-to-use-amazon-dynamodb-global-tables-to-power-multiregion-ar

NO.30 A Solution Architect is investigating purchasing options for a batch processing application on Amazon EC2 The batch job downloads an image from an Amazon S3 bucket, adds copyright information and uploads it back to Amazon S3, it normally takes 5 to 10 hours process all the files uploaded each week The application has built-in capabilities to process files in parallel, recover from the instance and continue the processing from where it left off.

What is the MOST cost-effective purchasing option the Solutions Architect can recommend?

A. Standard Reserved Instances

B. Scheduled Reserved Instances

C. Spot Instances

D. On-Demand Instances

Answer: C

NO.31 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

Answer: C

NO.32 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.

Answer: A
Explanation
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html

NO.33 As part of a migration strategy, a Solutions Architect needs to analyze 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.

Answer: D

NO.34 A Solutions Architect must design an Amazon DynamoDB table to store data about customer activities. The data is used to analyze recent customer behavior, 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.
Answer: C E
Explanation
https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-importexport-ddb-pipelinejson-verifydata2.
https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/best-practices.html

NO.35 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, an 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.
Answer: A D

NO.36 A Company wants to design a web application on stateless web servers in an Auto Scaling group.
How can sensitive user data be handled to ensure a stateless design based on best practices.?
A. Use cookies with the web server to store user data and session state on the client
B. Use Amazon DynamoDB for user data and cookies on the client to store session state
C. Use Amazon SQS to make the workloads stateless and track execution history
D. Use the ephemeral storage on the instances to store session state and Amazon DynamoDB for user data
Answer: D

NO.37 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 fulfills 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.

Answer: D

Explanation
When we perform the RAID 0 Striping of multiple volumes, IOPS are distributed among the volumes of a stripe. If you add another volume to RAID 0, you get the straight addition of IOPS throughput of that volume and additional volume size. Reference:
https://cloudacademy.com/blog/amazon-aws-raid-0-configuration-on-ebs-volumes/

NO.38 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.

Answer: B

NO.39 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.

Answer: C

Explanation
https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/

NO.40 An organization has a 3-tier architecture. It uses an Apache web server and an application is running on the Docker platform with Amazon RDS on the backend. The organization wants to migrate the application to AWS and does not want to be responsible for deployment scalability, or capacity provisioning of its resources.
Which service should be used to meet these requirements?
A. AWS OpsWorks
B. Amazon EC2 Elastic Container Service
C. AWS Elastic Beanstalk
D. AWS CloudFormation
Answer: B

NO.41 An Amazon DynamoDB table receives 1,000 transactions each day. A batch job must process these transactions after 8:00 p.m. each night to generate and email invoice to customers. It takes up to 5 second to process a single transaction.
How should A Solutions Architect design a solution to process the transaction each night?
A. Schedule AWS Glue to process the transactions from the DynamoDB table each night
B. Script the nightly launch of an Amazon EC2 instance with an application that processes the transactions.
C. Configure an Amazon DynamoDB Stream on the DynamoDB table to trigger an AWS Lambda function for each transaction.
D. Schedule a single invocation of an AWS Lambda function to sequentially process all transactions each night
Answer: B

NO.42 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
Answer: D
Explanation
https://medium.com/awesome-cloud/aws-difference-between-sqs-and-sns-61a397bf76c5

NO.43 A medical office has a requirement to store data for seven years. The data is stored in

AmazonS3, but they do not have a large budget for storing this data and do not plan on accessing the data unless audited.
What is the MOST cost-efficient, secure, and redundant solution for this scenario?
A. Copy the data to an Amazon EFS volume and mount it to six instances in a VPC
B. Export the data from AmazonS3 with AWS Snowball and store the data on a local RAID 1 Array
C. Use AmazonS3 Lifecycle policies to transition the data to S3-IA and then to Amazon Glacier
D. Periodically download the data to an Amazon EBS volume and archive the data to Amazon Glacier
Answer: C

NO.44 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 oneway 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.
Answer: D

NO.45 A company's new web application running on Amazon EC2 across multiple Availability Zones (AZs) will be heavily accessed during regular business hours After business hours, usage will be minimal. What fleet-scaling approach should be used to size the EC2 fleet to handle the traffic demands?
A. Manual scaling across all AZs
B. Provisioning for peak traffic
C. Scheduled scaling
D. Programmatic termination of all instances in one AZ during off-peak hours
Answer: C

NO.46 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
Answer: D E

Explanation
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-architecture.html

NO.47 A company hosts its website on Amazon S3. When a new version of the websites is released, a new set of files is used, and the previous version is archived. For regulatory and audit reasons, all the files used for the website must be kept for seven years. If auditor needs to retrieve a file. It must be available within four days.
Which is the MOST cost-effective storage option to store backup files?
A. Amazon EBS
B. Amazon S3 Standard
C. Amazon S3 IA
D. Amazon Glacier
Answer: D

NO.48 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
Answer: A
Explanation
https://aws.amazon.com/api-gateway/
The best solution would be to convert the code for the API and use it in a Lambda function. This can help save on cost, since in the case of Lambda, you only pay for the time the function runs, and not for the infrastructure.
Then, you can use the API Gateway along with the AWS Lambda function to scale accordingly. For more information on using API Gateway with AWS Lambda, please visit the following URL:
https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-with-lambda-integration.html

NO.49 A solutions Architect is designing a web application that contains an Auto scaling group with AmazonEC2 instances behind an Elastic Load Balancing load balancer. The EC2 instances access static content within an AmazonS3 bucket. When application load reaches a specified threshold, the Auto scaling group will scale up and deploy new EC2 instances to handle the additional load.
When new EC2 instances are deployed using the Auto scaling group, what should the Architect do to ensure that the instances can access static content within the S3 bucket?
A. Configure the Auto scaling group to launch instances with an AWS IAM role with readonly permissions to the S3 bucket
B. Create a security group that grants AmazonS3 read-only permissions for instances behind the load

balancer and apply it to the S3 bucket

C. Apply an AWS IAM policy to the S3 bucket that permits read-only access the folder 'staticcontent' from the EC2 instances

D. Create an AWS IAM user with a policy that grants the permissions to read the S3 bucket. Configure the load balancer to store the user's Public/Private key.

Answer: A

NO.50 An application is used to process customer orders using an Amazon EC2 instance which saves the orders to an Amazon Aurora database. Occasionally, when traffic is high, the workload does not process orders fast enough.

What will ensure that the orders are written to the database as quickly as possible?

A. Use an Application Load Balancer and an auto scaling group to distribute the load across multiple instances. Write orders to an Amazon SQS queue. Use EC2 instances in an Auto scaling group to read from the SQS queue and process orders into the database.

B. Increase the instance size of the web server when traffic is high. Write orders as messages to Amazon SNS, ensuring the database is subscribed to the SNS topic.

C. Use an Application Load Balancer and an auto scaling group to distribute the load across multiple instances. Write orders to an Amazon SQS queue. When instances have spare CPU available, read from the SQS queue and process orders into the database

D. Use an Application Load Balancer and an auto scaling group to distribute the load across multiple instances. Write orders as messages to SNS, ensuring that the database is subscribed to the SNS topic.

Answer: A

NO.51 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.

Answer: D

Explanation

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

NO.52 A company creates business-critical 3D images every night. The images are batchprocessed 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
Answer: B

NO.53 A large enterprise has highly sensitive customer data which is stored in several Amazon S3 buckets.
Which of the following features should be enabled to detect unauthorized access to the buckets?
A. Amazon VPC flow logs
B. Amazon CloudWatch Logs
C. Amazon S3 server access logs
D. AWSCloudTrail
Answer: D

NO.54 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
.
Answer: D
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

NO.55 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.
Answer: C

NO.56 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.

Answer: D

Explanation

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

NO.57 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 Amazoncloudwatch logs for all AWS services across all regions and aggregate them in a single 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.

Answer: D

NO.58 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

C. ELB Classic Load Balancer

D. Amazon RDS

Answer: B

Explanation

https://aws.amazon.com/articles/high-availability-for-amazon-vpc-nat-instances-an-example/

Instances in a private subnet can access the Internet without exposing their private IP address by routing their traffic through a Network Address Translation (NAT) instance in a public subnet. A NAT instance, however, can introduce a single point of failure to your VPC's outbound traffic. This situation is depicted in the diagram below.

NO.59 An organization uses an AWS development account and a production account. In each account there is exactly one Amazon VPC that is in the same AWS region. The organization needs to allow traffic to be routed between these two VPC without going out of the AWS network infrastructure.

Which service should be used to meet this requirements?

A. A virtual private gateway

B. AWS VPN CloudHub

C. VPC peering

D. AWS Direct Connect

Answer: C

NO.60 A web application has an increase in traffic during certain times of the day, and a Solutions Architect notices that CPU usage reaches 100%, which results in poor application performance.
How should the solutions Architect ensure that adequate compute resources are provisioned at all times?

A. Launch Spot Instances when CPU exceeds a given threshold

B. Use Elastic Load Balancing to balance the load during high-traffic periods

C. Use Amazon EC2 Auto Scaling to launch instances when CPU exceeds a given threshold

D. Purchase Reserved Instances to ensure capacity

Answer: C

NO.61 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

Answer: A
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html
"This scenario can also be optionally configured for IPv6-you can use the VPC wizard to create a VPC and subnets with associated IPv6 CIDR blocks. Instances launched into the subnets can receive IPv6 addresses, and communicate using IPv6. Instances in the private subnet can use an egress-only Internet gateway to connect to the Internet over IPv6, but the Internet cannot establish connections to the private instances over IPv6. For more information about IPv4 and IPv6 addressing, see IP Addressing in Your VPC."

NO.62 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 analyze the queries.

C. Integrate Amazon ElastiCache into the application.

D. Use a Lambda-triggered request to the backend database.

Answer: C
Explanation
https://aws.amazon.com/blogs/database/automating-sql-caching-for-amazon-elasticache-and-amazon-rds/

NO.63 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 of 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 from the IP addresses of the LC2 instances only to accept 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 Die Auto Scaling group Set the destination to the security group associated with the RDS database instance
D. Configure the inbound network ACLs on the da only from the CIDR range of the subnet used by subnet Auto Scaling group
Answer: C

NO.64 Before approving the use of AWS for a new application, the infosec team has asked if it will be possible for specific IP addresses to be blocked from accessing the application, in the event that a threat is detected from a particular block of IP addresses on the internet.
What could be used to meet this requirement?
A. Network Access control lists
B. Security groups
C. Virtual Private Gateways.
D. Internet Gateways
Answer: A

NO.65 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
Answer: B

NO.66 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

Answer: B

Explanation

Amazon DynamoDB transactions simplify the developer experience of making coordinated, all-or-nothing changes to multiple items both within and across tables. Transactions provide atomicity, consistency, isolation, and durability (ACID) in DynamoDB, enabling you to maintain data correctness in your applications easily.

Refer pdf -Page 629

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/dynamodb-dg.pdf

NO.67 A hotel management application generates logs whenever an electronic room key is used on a door lock, indicating whether the entry request was granted or rejected. After a number of rejected entries exceeds an average of one per minute. The notification should be received within a few minutes of the rate being exceeded.

How should a solutions Architect design a solution to meet this requirement without making any code changes?

A. Sand events to an Amazon Kinesis Data stream. Write a Kinesis client library application to consume the events count rejections and send a message to Amazon SNS for notifications.

B. Send the logs to Amazon CloudWatch Logs Filter for rejections Create an alarm when the rate is exceeded Use Amazon SNS for notifications

C. Send events to an Amazon SQS queue that is configured to trigger an AWS Lambda function If the rate is exceeded. Lambda sends a message to Amazon SNS for notifications

D. Send logs directly to Amazon SNS with a granted rejected flag as a message attribute Use a subscription filter policy to send only rejection notifications

Answer: B

NO.68 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.

Answer: C

NO.69 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 while 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 At-S-256
C. Configure S3 object encryption using AWS CI I with Server Side Enciyption with AWS KMS Managed Keys (SSL KMS)
D. Configure S3 buckets to use Server Side Encryptjon with AWS KMS-Managed Keys (SSF-KMS) with imported key material in both regions
Answer: A

NO.70 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.
Answer: C

NO.71 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
Answer: A
Explanation
https://cloud.netapp.com/blog/2015/amazon/demystifying-amazon-web-services-an-enterprise-

admins-view-of-th

NO.72 A Solutions Architect is designing a solution that retains traffic information between network interfaces. This traffic information will then be monitored for anomalies by an Infosec team using Amazon CloudWatch.
What approach should the architect take?
A. Save all inbound requests to Amazon DynamoDB
B. Maintain traffic history on each Amazon EC2 instance
C. Enable Amazon VPC Flow Logs.
D. Save all inbound requests to Amazon S3
Answer: C

NO.73 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
Answer: B

NO.74 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
Answer: B
Explanation
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html#georestrictions-clo

NO.75 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.

Answer: C

Explanation

https://medium.com/@matthewleak/aws-lambda-functions-with-a-static-ip-89a3ada0b471

https://aws.amazon.com/premiumsupport/knowledge-center/internet-access-lambda-function/

NO.76 A Solutions Architect must select the most cost-efficient 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

Answer: C

Explanation

Initial Concurrency Burst Limits

3000 - US West (Oregon), US East (N. Virginia), EU (Ireland).

1000 - Asia Pacific (Tokyo), EU (Frankfurt).

500 - Other regions.

NO.77 A Solutions Architect is migrating a company's MySQL database to an Amazon RDS MySQL database. The company requires the database to be resilient with minimum downtime when failures occur.

How can these requirements be met?

A. Enable a read replica in another Availability Zone

B. Enable multiple Availability Zones in a different AWS Region

C. Enable multiple Availability Zones in a same AWS Region

D. Enable Amazon RDS instance snapshots in one Availability Zone

Answer: C

NO.78 A client is building a payment processing service that sends orders to a fulfilment service. Both these services have varying levels of throughput. What can the client use to decouple requests between these components to better handle burst traffic during peak holiday season?

A. Use Amazon SQS to send messages between the two services

B. Set up the services in separate AWS regions

C. Use Amazon Redshift for sending orders to the fulfilment service

D. Setup internal Elastic Load Balancer for synchronous calls between the two services.

Answer: A

NO.79 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
Answer: D
Explanation
https://aws.amazon.com/blogs/aws/cross-region-snapshot-copy-for-amazon-rds/ You can enable point-in-time recovery using the AWS Management Console, AWS Command Line Interface (AWS CLI), or the DynamoDB API. When it's enabled, point-in-time recovery provides continuous backups until you explicitly turn it off.
After you enable point-in-time recovery, you can restore to any point in time within EarliestRestorableDateTime and LatestRestorableDateTime. LatestRestorableDateTime is typically 5 minutes before the current time.
Availability Zones:
With their own power infrastructure, the AZs are physically separated by a meaningful distance, many kilometers, from any other AZ, although all are within 100 km (60 miles of each other)
https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
Large scale disaster recovery using AWS regions
DR takes things to a completely new level, wherein you need to be able to recover from a different region that's separated by over 250 miles
https://aws.amazon.com/blogs/startups/large-scale-disaster-recovery-using-aws-regions/

NO.80 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 Firehouse and Amazon S3
C. Amazon ECS and Amazon RDS
D. Amazon S3 events and AWS Lambda
Answer: D

NO.81 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

Answer: D
Explanation
https://aws.amazon.com/blogs/aws/scalable-session-handling-in-php-using-amazon-dynamodb/

NO.82 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.
E. Have a standby Amazon RDS instance in a separate Availability Zone.
Answer: C D

NO.83 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
Answer: C
Explanation
https://aws.amazon.com/blogs/database/how-to-configure-a-private-network-environment-for-amazon-dynamodb

NO.84 A company has a web application that makes requests to a backend API service. The API service is behind an Elastic Load Balancer running on Amazon EC2 instances.
Most backend API service endpoint calls finish very quickly, but one endpoint that makes calls to create objects in an external service takes a long time to complete These long-running calls are causing client timeouts and increasing overall system latency What should be done to minimize the system throughput impact of the slow-running endpoint?
A. Change the EC2 instance size to increase memory and compute capacity
B. Use Amazon SQS to offload the long-running requests for asynchronous processing by separate workers.
C. Increase the load balancer idle timeout to allow the long-running requests to complete.
D. Use Amazon ElastiCache for Redis to cache responses from the external service.
Answer: D

NO.85 A new application is being deployed on AmazonEC2. The Application needs to read write upto 3 TB of data to an external data store and requires read-after-write consistency across all AWS regions for writing new objects into this data store.
Which is the most cost-effective data storage service that meets these requirements?

A. Amazon EBS
B. Amazon Glacier
C. Amazon EFS
D. AmazonS3
Answer: D

NO.86 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.
A. Which storage solution meets the needs of this organization while providing the LOWEST cost of storage?
B. Store the archive in Amazon S3 Reduced Redundancy Storage.
C. Store the archive in Amazon Glacier and use standard retrieval for all content.
D. Store the archive in Amazon Glacier and pay the additional charge for expedited retrieval when needed.
E. Store the archive in Amazon S3 with a lifecycle policy to move this to S3 Infrequent Access after 30 days
Answer: C

NO.87 A customer has a legacy application with a large amount of data. The files accessed by the application are approximately 10 GB each, but are rarely accessed. However, when files are accessed, they are retrieved sequentially. The customer is migrating the application to AWS and would like to use Amazon EC2 and Amazon EBS.
What is the LEAST expensive EBS volume type for this use case?
A. Cold HDD (sc1)
B. Provisioned IOPS SSD (io1)
C. General Purpose SSD (gp2)
D. Throughput Optimized HDD (st1)
Answer: A
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

NO.88 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
Answer: C
Explanation
https://docs.aws.amazon.com/en_pv/elasticloadbalancing/latest/application/introduction.html#appl

ication-load-b Support for containerized applications. Amazon Elastic Container Service (Amazon ECS) can select an unused port when scheduling a task and register the task with a target group using this port. This enables you to make efficient use of your clusters. Support for path-based routing. You can configure rules for your listener that forward requests based on the URL in the request. This enables you to structure your application as smaller services, and route requests to the correct service based on the content of the URL.
https://docs.aws.amazon.com/aws-technical-content/latest/microservices-on-aws/microservices-on-aws.pdf?icmp

NO.89 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 a 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.
Answer: A

NO.90 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
Answer: B
Explanation
What Is Amazon Kinesis Data Firehose?
Amazon Kinesis Data Firehose is a fully managed service for delivering real-time streaming data to destinations such as Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Elasticsearch Service (Amazon ES), and Splunk. Kinesis Data Firehose is part of the Kinesis streaming data platform, along with Kinesis Data Streams, Kinesis Video Streams, and Amazon Kinesis Data Analytics. With Kinesis Data Firehose, you don't need to write applications or manage resources. You configure your data producers to send data to Kinesis Data Firehose, and it automatically delivers the data to the destination that you specified. You can also configure Kinesis Data Firehose to transform your data before delivering it

NO.91 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
Answer: D
Explanation
https://www.edureka.co/community/2813/aws-autoscaling-without-elastic-load-balancing

NO.92 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. 1AM database authentication
D. VPC security group for Redis
Answer: A

NO.93 A mobile client requires data from several application- layer services to populate its user interface.
What can the application team use to decouple the3 client interface from the underlying behind them?
A. Application load balancer
B. Amazon API gateway
C. Amazon cognito
D. AWS device farm
Answer: D

NO.94 A Solution Architect must design a monitoring solution that gives the Security team visual access to all Amazon S3 bucket-level API operations.
What should the Solution Architect use to provide this information?
A. AWS CloudTrail logging for management events
B. Amazon CloudWatch Logs
C. AWS CloudTrail logging for data events
D. S3 Server Access logging
Answer: C

NO.95 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 URL's Design a Lambda function to remove data that is older than 14 days.
B. Use an S3 bucket and provide direct access to the tile Design the application to track purchases in a DynamoDH 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 sot 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

Answer: C

NO.96 A Solutions Architect must create a solution whereby user access to multiple Amazon Aurora MySQL databases is securely managed with short-lived connection credentials.
How can the Solutions Architect meet these requirements?

A. Create a database user to run the GRANT statement with a short-lived token.

B. Create the user account to use the AWS-provided AWSAuthenticationPlugin with IAM.

C. Use AWS Systems Manager to securely save the connection secrets, and use the secrets while connecting.

D. Use AWS KMS to securely save the connection secrets, and use the secrets while connecting.

Answer: B

Explanation

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/UsingWithRDS.IAMDBAuth.Connecting.ht With IAM database authentication, you use an authentication token when you connect to your DB cluster. An authentication token is a string of characters that you use instead of a password. After you generate an authentication token, it's valid for 15 minutes before it expires. If you try to connect using an expired token, the connection request is denied.

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/UsingWithRDS.IAMDBAuth.Connecting.A

"When you connect using AWSAuthenticationPlugin, the connection is secured using SSL. To verify this, type the following at the mysql> command prompt. "

NO.97 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

Answer: C

NO.98 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

Answer: A

Explanation

https://aws.amazon.com/caching/session-management/

NO.99 An Amazon EC2 instance has been running and data has been stored on the instance volumes. The instance was shut down over the weekend to save costs. The next week, after starting the instance, the Solution Architect found that all the data was lost and is no longer available on the instance.

What was the cause of this situation?

A. The Amazon EC2 instance was using instance store volumes

B. The Amazon EC2 instance was using Amazon EBS-backed root volumes.

C. The volume was not big enough to handle all of the data

D. The volume did not have sufficient IOPs.

Answer: A

NO.100 An organization wants to migrate a legacy Ruby-on Rails application to AWS. The application is not used frequently, but it must be scalable during peak use. The organization requires minimal code changes, if any, to the application.

Which of the following solutions will meet the organization's requirements for moving the application to AWS?

A. Migrate the application to AWS Lambda.

B. Deploy the application to an EC2 instance.

C. Host the application on Amazon S3, and use Amazon CloudFront to cache static assets.

D. Create an AWS Elastic Beanstalk deployment for the application with satisfactory scaling criteria.

Answer: D

NO.101 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

Answer: A

Explanation

https://aws.amazon.com/cloudfront/features/

NO.102 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.
Answer: A C

NO.103 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 fulfill 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.
Answer: D
Explanation
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-simple-configs.html

NO.104 An on-premises workload consists of a single server with an Apache instance and a MYSQL database. The Solutions Architect plans to migrate the on-premises database to MYSQL on Amazon RDS using multiple Availability Zones.
What solution ensure that the remaining workload will be highly available?
A. Provision the workload in an Auto Scaling group, with a minimum of two servers Use an Amazon Route
53 DNS-weighted routing policy to direct traffic to healthy servers.
B. Provision the workload in an Auto Scaling group across Availability Zones with a minimum of two Amazon EC2 instances Use an Application Load Balancer in front of an Auto Scaling group
C. Provision at least two EC2 instances across two separate regions Use an Application Load Balancer to direct traffic between the instances.
D. Provision the workload in an Auto Scaling group across Availability Zones, with a minimum of two servers. Use a Route 53 DNS simple routing policy to direct traffic to healthy servers
Answer: D

NO.105 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.

Answer: C E

Explanation

Both helps facilitate infrastructure management and deployment. Check out this article on "Why Use AWS Lambda in a Custom VPC?": https://aws.amazon.com/blogs/apn/why-use-aws-lambda-in-a-custom-vpc/

NO.106 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

Answer: A

Explanation

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

NO.107 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 1AM 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 1AM users in each account.

Answer: C

Explanation

https://aws.amazon.com/premiumsupport/knowledge-center/iam-policy-service-control-policy/

NO.108 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
Answer: B

NO.109 To meet the requirements of an application, an organization needs to save a constantly increasing volume of files on a cloud storage system with the following features and abilities:
Pay only for the storage used
Create different security policies for different groups of files
Allow access to the public
Retrieve the files at any time
Store an unlimited number of files
What AWS service will meet these requirements?
A. Amazon EBS
B. Amazon S3
C. Amazon Glacier
D. Amazon EFS
Answer: B

NO.110 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 rearchitected.
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.
Answer: B
Explanation
https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html
Cached volumes - You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data. Stored volumes - If you need low-latency access to your entire dataset, first configure your on-premises gateway to store all your data locally. Then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive offsite backups that you can recover to your local data center or Amazon EC2. For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2
https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

NO.111 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
Answer: A C
Explanation
Amazon Kinesis Data Firehouse --Amazon Kinesis Analytics allows you to process streaming data coming from IoT devices in real timE Amazon Redshift--Amazon Redshift is a fast, fully managed, and cost-effective data warehouse that gives you petabyte scale data warehousing and exabyte scale data lake analytics together in one service

NO.112 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.
Answer: C
Explanation
(https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-deli

NO.113 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
Answer: D
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html

NO.114 A customer is running a critical payroll system in a production environment in one data center and a disaster recovery (DR) environment in another. The application includes load-balanced web servers and failover for the MySQL database. The customer's DR process is manual and error-

phone. 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.

Answer: D

NO.115 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.

Answer: C
Explanation
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

NO.116 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.

Answer: C

Explanation

https://aws.amazon.com/ecs/features/

NO.117 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.

Answer: D

Explanation

https://docs.aws.amazon.com/efs/latest/ug/creating-using.html

Creating Resources for Amazon EFS Amazon EFS provides elastic, shared file storage that is POSIX-compliant. The file system you create supports concurrent read and write access from multiple Amazon EC2 instances and is accessible from all of the Availability Zones in the AWS Region where it is created.

NO.118 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

Answer: C

Explanation

https://aws.amazon.com/elasticbeanstalk/

NO.119 A company is building a critical ingestion service on AWS that will receive 1,000 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

Answer: A
Explanation
Q: How does Amazon Kinesis Data Streams differ from Amazon SQS? Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering). Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows.

NO.120 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
Answer: A
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/

NO.121 A solutions Architect needs a storage solution for a fleet of Linux web application servers. The solution should provide the system interface and be able to support millions of files.
Which AWS service should the architect choose?
A. AmazonS3
B. Amazon EFS
C. Amazon EBS
D. AmazonElasticache
Answer: B

NO.122 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.

Answer: C
Explanation
https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-Lab2cjLoX9c9IgJaCN8/Please
https://aws.amazon.com/rds/details/read-replicas/

NO.123 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 Solution Architect design a system to durably store the number of calls without requiring changes to the application?

A. Call the service through an internet a gateway.

B. Decouple application from the service with an Amazon SQS queue

C. publish a custom Amazon CloudWatch metric that counts calls to the service.

D. Call the service through VPC peering connection.

Answer: C
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-custom-metrics/

NO.124 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

Answer: B
Explanation
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-video.html

NO.125 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.

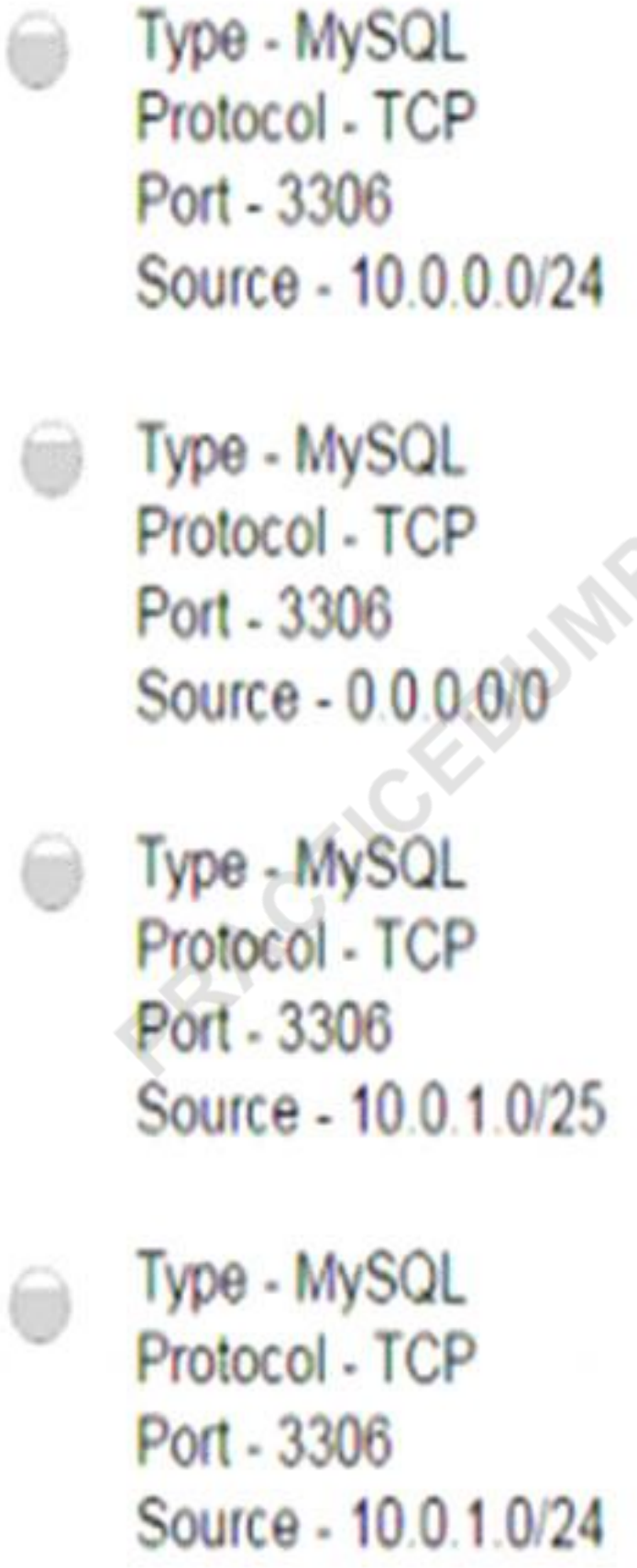
Answer: D

Explanation
https://aws.amazon.com/rds/details/read-replicas/ and
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

NO.126 A Solutions Architect is building an Amazon VPC and subnets in two Availability Zones to match a three-tier architecture. The IP addresses of the subnets are as follows:

	us-east-1a	us-east-1b
Web	10.0.0.0/25	10.0.0.128/25
Application	10.0.1.0/25	10.0.1.128/25
Data	10.0.2.0/25	10.0.2.128/25

The databases has sensitive information. For this reason, the Security team will allow only instances in the application tier to communicate with the data tier. No other access to the data tier is permitted.
Which of the following security groups meet the requirements for access to the data tier?



A. Option A
B. Option B
C. Option C

D. Option D
Answer: D

NO.127 An application is running in a single AWS region. The business team adds a requirement to run the application in a second region for multi-region high availability. A Solutions Architect needs to enable traffic to be distributed to multiple regions for high availability.
Which AWS service meets the requirements?
A. Amazon Route 53
B. Elastic Load Balancing
C. Amazon CloudFront
D. Amazon S3 Website Hosting
Answer: A

NO.128 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
Answer: D
Explanation
https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html

NO.129 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. Scale up to a larger RDS instance type.
B. Change the RDS database instance to multiple Availability Zones.
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.
Answer: B C

NO.130 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 longterm 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
Answer: A
Explanation

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

NO.131 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

Answer: B

Explanation
AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer.
https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

NO.132 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

Answer: B

Explanation
https://aws.amazon.com/blogs/big-data/building-and-maintaining-an-amazon-s3-metadata-index-without-servers

NO.133 A Solution Architect is developing as AWS Lambda-based service for a social networking game to retrieve information on tourist landmarks stored in an Amazon DynamoDB table. The solutions Architect wants to minimize costs as the service scales to many millions of users through a mobile app.
How can the Solution Architect optimize performance while minimizing costs? (Select TWO)

A. Use DynamoDB Accelerator (DAX), and configure Auto Scaling of read throughput on the DynamoDB table.

B. Configure AppSync to cache responses on the mobile client and configure Auto Scaling of reads on the DynamoDB table.

C. Configure Amazon CloudFront, specify an appropriate TTL for response caching, and configure the DynamoDB table as the origin.

D. Authorize mobile clients to communicate directly with DynamoDB through AWS STS tokens, and configure DynamoDB for global replication and Auto Scaling.

E. Expose the Lambda function through the Amazon API Gateway, configure the endpoint with caching, and configure Auto Scaling of read throughput on the DynamoDB table.

Answer: A E

NO.134 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
Answer: B

NO.135 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 fit to insert the item?
A. Lambda@Edge
B. AWS Lambda
C. Amazon API Gateway
D. Amazon EC2 instances
Answer: B
Explanation
https://aws.amazon.com/blogs/machine-learning/build-your-own-face-recognition-service-using-amazon-rekogn

NO.136 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.
Answer: D

NO.137 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
Answer: B

NO.138 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
D. Amazon S3 Standard
Answer: B

NO.139 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
Answer: B
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

NO.140 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 1AM policies restricting user access to specific time periods.
C. Use Amazon S3 with the default private access policy and generate presigned 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.
Answer: C

NO.141 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.
Answer: C
Explanation
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/monitoring-cloudwatch-vpn.html

NO.142 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
Answer: B
Explanation
You can use the cloudfront with Route 53 Geolocation Routing. But the location wise content delivery is already enabled in cloudfront, so geolocation policy wont help that much. If you are not using cloudfront and you want to distribute traffic based on user location, then you can use Route53

NO.143 A Solution Architect is creating a multi-tiered architecture for an application that includes a public-facing web tier. Security requirement state that the Amazon EC2 instance running in the application tier must not be accessible directly from the internet.
What should be done to accomplish this?
A. create a multi-VPC peering mesh with network access rules limiting Communications to specific ports implements an internet gateway on each VCP for external communication.
B. Place all instances in a single Amazon VPC with AWS WAF as the web front-end communication conduit Configure a NAT gateway for external communications.
C. Use VPC peering to peer with on-premises hardware. Direct enterprise traffic through the VPC peer connection to the instances hosted in the private VPC.
D. Deploy the web and application instances in a private subnet Provision an Application Load Balancer in the public subnet install gateway and use security groups to control communications between the layers.
Answer: D
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

NO.144 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

Answer: A E

NO.145 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

Answer: D

Explanation
https://aws.amazon.com/es/blogs/aws/new-vpc-endpoints-for-dynamodb/
https://aws.amazon.com/blogs/database/how-to-configure-a-private-network-environment-for-amazon-dynamodb

NO.146 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.

Answer: C

Explanation
Amazon CloudFront is a content delivery network offered by Amazon Web Services. Content delivery networks provide a globally-distributed network of proxy servers which cache content, such as web videos or other bulky media, more locally to consumers, thus improving access speed for downloading the content

NO.147 A solutions Architect is building a new feature using 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 EFS

Answer: B

NO.148 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

Answer: B

Explanation
https://aws.amazon.com/blogs/startups/how-to-accelerate-your-wordpress-site-with-amazon-cloudfront/

NO.149 A company needs to use AWS resources to expand capacity for a website hosted in an onpremises 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.

Answer: A B

Explanation
https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-ba
Q. Can I point my zone apex (example.com versus www.example.com) at my Elastic Load Balancer?
Yes. Amazon Route 53 offers a special type of record called an 'Alias' record that lets you map your zone apex (example.com) DNS name to the DNS name for your ELB load balancer (such as my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com). IP addresses associated with load balancers can change at any time due to scaling up, scaling down, or software updates. Route 53 responds to each request for an Alias record with one or more IP addresses for the load balancer. Route 53 supports alias records for three types of load balancers: Application Load Balancers, Network Load Balancers, and Classic Load Balancers.

There is no additional charge for queries to Alias records that are mapped to AWS ELB load balancers. These queries are listed as "Intra-AWS-DNS-Queries" on the Amazon Route 53 usage report.

NO.150 A customer needs to provide full access to the objects stored in an Amazon S3 bucket, but only for the members of the HR department.
How can a Solutions Architect meet this requirement with the LEAST administrative overhead?
A. Configure Amazon S3 preassigned URLs for the objects stored in the bucket for members of the HR department.
B. Configure a policy for the HR department IAM group to allow full accessions bucket
C. Configure server-side encryption win Amazon S3-Managed Keys (SSE-S3) for the bucket
D. Configure S3 bucket ACLs to grant the required permissions in the bucket for members of the HR department
Answer: D

NO.151 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
Answer: C
Explanation
https://aws.amazon.com/about-aws/whats-new/2019/02/amazon-sqs-fifo-qeues-now-available-in-15-aws-regions

NO.152 A Solutions Architect has an application running on an Amazon EC2 instance in a VPC. A client running in another VPC in the same region must be able to communicate with this application. Security policies require that this application should not be accessible from the internet.
Which architectures will meet these requirements? (Select TWO)
A. Configure a VPC peering connection between the application VPC and the client VPC.
B. Configure an Elastic Load Balancing (ELB) Network Load Balancer as a VPC endpoint in the application VPC, connect to it from the clients' VPC
C. Configure AWS Direct Connect and private virtual interface between the application VPC and the client VPC
D. Configure a NAT gateway in the VPC in the application VPC
E. Configure an egress-only internet gateway in the application VPC
Answer: A B

NO.153 A Company has a legacy application using a proprietary file system and plans to migrate the application to AWS.
Which storage should the company use?

A. Amazon Dynamo DB
B. Amazon S3
C. Amazon EBS
D. Amazon EFS
Answer: D

NO.154 A company stores website images in Amazon S3 and wants to automatically create thumbnails from them. A Solutions Architect must create a highly scalable infrastructure to store and execute thumbnail-creation code.
The Solutions Architect wants to use Amazon S3 event notification to accomplish this task.
Which service should the Solutions Architect choose to trigger from the event?
A. Amazon API Gateway
B. AWS Lambda
C. Amazon Redshift
D. AWS Batch
Answer: B

NO.155 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.
Answer: C
Explanation
From https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock.html S3 Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual S3 Glacier vaults with a vault lock policy. You can specify controls such as "write once read many" (WORM) in a vault lock policy and lock the policy from future edits. Once locked, the policy can no longer be changed. S3 Glacier enforces the controls set in the vault lock policy to help achieve your compliance objectives, for example, for data retention. You can deploy a variety of compliance controls in a vault lock policy using the AWS Identity and Access Management (IAM) policy language.

NO.156 A Solutions Architect is designing a disaster recovery (DR) environment in a separate AWS region from an application's primary workload. The application uses a multi-tier architecture, and only the RDS instance will have frequent changes. The application installation process takes 60 minutes on average. The disaster recovery plan must have an RPO of less than 90 minutes and an RTO of less than 30 minutes.
Which of the following would enable the Solutions Architect to meet these requirements? (Select TWO.)
A. An Aurora instance as the primary database with a read replica in the DR region

B. Inter-region VPC peering between the primary workload VPC and the DR VPC
C. A cross-region Amazon EC2 Amazon Machine Image (AMI) copy
D. Amazon S3 cross-region replication of application-tier installers
E. Amazon Cloud Watch Events in the primary region that trigger the failover to the DR region
Answer: A C
Explanation
https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-KMGyLGiwynhaPzFXf7Z/wh

NO.157 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 (1AM) 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 (1AM) 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 (1AM) role allowing access from AWS Lambda and assign the role to the DynamoDB table.
Answer: A
Explanation
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.

NO.158 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 WriteThrough 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.
Answer: D
Explanation
https://www.tutorialspoint.com/awselasticache/awselasticache_write_through

NO.159 A Solutions Architect is working with an infrastructure that consists of multiple Amazon EC2 application and web servers. The Architect needs to be able to meet demand for an expected spike in traffic to the website.
How can the Architect ensure high availability and durability?
A. Placement groups and Amazon CloudFront
B. Auto scaling and Elastic Load Balancing
C. AWS CloudFormation and Amazon CloudFront
D. Elastic Load Balancing and AWS CloudFormation
Answer: B

NO.160 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.
Answer: A

NO.161 A customer has an application that is hosted in the AWS us-west-2 region with users across the United States.
Users on the East Coast of the United States are complaining that the user interface takes a long time to load time to load but that once loaded, the application generally performs well. The one exception is when loading large common data views, such as account listings and auto- complete queries. Users on the West Coast do not report these issues. The company is concerned about the performance of East Coast users and for an upcoming launch in the European market.
What change can a Solutions Architect make to the architecture to solve the performance problems for users in the eastern United States and the upcoming European market without impacting existing users?
A. Move the application servers and data to the us-east-1 region to decrease latency to the East Coast and European users
B. Deploy a set of the proxy servers in the us-east-1 and eu-west-1 regions to serve stake content
C. Place the application servers behind an Amazon CloudFront distribution
D. Move the static assets to Amazon S3 and place the S3 bucket behind an Amazon CloudFront distribution
Answer: D

NO.162 A Solutions Architect is designing the architecture for a new three-tier web-based ecommerce 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.
B. Store all static files in a multi-AZ Amazon Aurora database.
C. Create an CloudFront distribution pointing to static content in Amazon S3.
D. Use Amazon Route 53 to route traffic to the correct region.
E. Use Amazon S3 multi-part uploads to improve upload times
Answer: A C

NO.163 A Solutions Architect needs to design an Amazon RDS for MySQL solution whereby users must be authenticated using only SSL connections.
How should the Solutions Architect design the solution?
A. Only allow SSL connections through a VPC security group
B. Use grant and alter commands with the require SSL option for the user
C. Connect with a MySQL client that references the public key
D. Ensure that the SSL parameters are set in the parameter group at launch
Answer: B

NO.164 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.
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.
Answer: A
Explanation
https://aws.amazon.com/blogs/aws/automated-cross-region-snapshot-copy-for-amazon-redshift/

NO.165 A Solutions Architect is building an Amazon ECS-based web application that requires that headers are not modified when being forwarded to Amazon ECS.
Which load balancer should the Architect use?
A. Application Load Balancer
B. Network Load Balancer
C. A virtual load balancer appliance from AWS marketplace
D. Classic Load Balancer
Answer: A

NO.166 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

Answer: C

NO.167 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.

Answer: C

Explanation

Expedited - Expedited retrievals allow you to quickly access your data when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using Expedited retrievals are typically made available within 1-5 minutes. Provisioned Capacity ensures that retrieval capacity for Expedited retrievals is available when you need it. For more information, see Provisioned Capacity.

Standard - Standard retrievals allow you to access any of your archives within several hours. Standard retrievals typically complete within 3-5 hours. This is the default option for retrieval requests that do not specify the retrieval option.

Bulk - Bulk retrievals are Glacier's lowest-cost retrieval option, which you can use to retrieve large amounts, even petabytes, of data inexpensively in a day. Bulk retrievals typically complete within 5-12 hours.

NO.168 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

Answer: B

NO.169 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.

Answer: A

Explanation

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-manage-subnets.html

NO.170 Application servers currently deployed in a private subnet require the ability to integrate with a third-party service accessible through the Internet.

Which changes are required to provide outbound Internet connectivity in the VPC without providing inbound Internet connectivity to the application servers?

A. Create a NAT Gateway without attaching an Internet Gateway to the VPC.

B. Create a NAT Gateway and attach an Internet Gateway to the VPC.

C. Attach an Internet Gateway to the VPC without creating a NAT Gateway.

D. Attach a Virtual Private Gateway to the VPC and create a NAT Gateway.

Answer: B

Explanation

NAT Gateway Basics

To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. For more information about public and private subnets, see Subnet Routing. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point Internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet.

Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone.

You have a limit on the number of NAT gateways you can create in an Availability Zone. For more information, see Amazon VPC Limits.

Note

If you have resources in multiple Availability Zones and they share one NAT gateway, in the event that the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

If you no longer need a NAT gateway, you can delete it. Deleting a NAT gateway disassociates its Elastic IP address, but does not release the address from your account.

The following diagram illustrates the architecture of a VPC with a NAT gateway. The main route table sends internet traffic from the instances in the private subnet to the NAT gateway. The NAT gateway sends the traffic to the internet gateway using the NAT gateway's Elastic IP address as the source IP address.

NO.171 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.

Answer: B

Explanation

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

NO.172 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 1AM 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.

Answer: B

NO.173 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

Answer: A

NO.174 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

Answer: B

Explanation

https://aws.amazon.com/about-aws/whats-new/2019/09/elastic-load-balancing-network-load-

balancers-now-supp
https://amazonaws-china.com/blogs/aws/new-application-load-balancer-sni/

NO.175 An organization is planning a migration from on-premises workloads to AWS, and needs a design that will provide greater operational transparency.
Which service should be built into the architecture to automate the capture and publishing of custom metrics that will provide this required transparency?
A. Amazon CloudWatch
B. AWS CloudTrail
C. AWS Developer Tools
D. AWS X-Ray
Answer: B

NO.176 A Solutions Architect is designing a high-performance computing job that runs on Amazon EC2 instances in private subnets. To allow the application to download patches, the infrastructure must be altered to allow the instances to access external endpoints. Any changes to the infrastructure must involve minimal ongoing systems management effort.
What will allow the EC2 instances to access the endpoint while meeting these requirements?
A. NAT gateway
B. Elastic IP address
C. AWS Direct Connect
D. Virtual private gateway
Answer: A
Explanation
Connect to the Internet using Network Address Translation (private subnets) - Private subnets can be used for instances that you do not want to be directly addressable from the Internet. Instances in a private subnet can access the Internet without exposing their private IP address by routing their traffic through a Network Address Translation (NAT) gateway in a public subnet.

NO.177 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
Answer: D

NO.178 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.
Answer: B
Explanation
In a Multi AZ, AWS runs just one DB but copies the data synchronously to the standby replica The question targets Read Contention(responsiveness) and write is not an issue and hence the Read Replicas.

NO.179 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.
Answer: A D
Explanation
https://docs.aws.amazon.com/sns/latest/dg/mobile-push-send-register.html
"For Amazon SNS to send notification messages to mobile endpoints, whether it is direct or with subscriptions to a topic, you first need to register the app with AWS. To register your mobile app with AWS, enter a name to represent your app, choose the platform that will be supported, and provide your credentials for the notification service platform. After the app is registered with AWS, the next step is to create an endpoint for the app and mobile device. The endpoint is then used by Amazon SNS for sending notification messages to the app and device."

NO.180 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 fulfill 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

Answer: D

Explanation

https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html In Amazon Redshift, you can enable database encryption for your clusters to help protect data at rest. When you enable encryption for a cluster, the data blocks and system metadata are encrypted for the cluster and its snapshots.

You can enable encryption when you launch your cluster, or you can modify an unencrypted cluster to use AWS Key Management Service (AWS KMS) encryption

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

NO.181 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

Answer: D

Explanation

https://aws.amazon.com/about-aws/whats-new/2018/09/amazon-s3-announces-selective-crr-based-on-object-tags

NO.182 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.

Answer: B

Explanation

https://docs.aws.amazon.com/en_pv/redshift/latest/mgmt/security-server-side-encryption.html

NO.183 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
Answer: A C

NO.184 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
Answer: A E

NO.185 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.
Answer: B C
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html

NO.186 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.
Answer: A E
Explanation

https://aws.amazon.com/premiumsupport/knowledge-center/iam-authentication-api-gateway/

NO.187 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.

Answer: B
Explanation
https://docs.aws.amazon.com/sns/latest/dg/sns-common-scenarios.html

NO.188 An online retailer is designing a public-facing web application with database servers that are not publicly accessible.
Which design is a secure way to ensure that the database have access to the internet to download security patches?

A. The web servers should be in a public subnet. The database servers should be in the private subnet with a route to a NAT gateway in the public subnet

B. The web servers should be in the private subnet with a route to the NAT gateway in the public subnet.
The database servers should be in the public subnet

C. The web servers and database servers should be in the private subnet with a route to a NAT gateway in the private subnet

D. The web servers and database servers should be in the public subnet with a route to a NAT gateway in the private subnet

Answer: C

NO.189 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

Answer: D
Explanation

https://aws.amazon.com/getting-started/projects/deploy-nodejs-web-app/

NO.190 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.

Answer: D

Explanation
Amazon S3--static files Amazon CloudFront-user experience AWS Lambda -serverless computing platform Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale DynamoDB -Session

NO.191 A Solutions Architect is defining 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

Answer: C

Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/bucket-policy-encryption-s3/

NO.192 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 1AM role with least privilege.

B. Create an 1AM policy granting access to all services and assign it to the Amazon EC2 instance profile.

C. Create an 1AM 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.

Answer: C

NO.193 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.
Answer: C
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html

NO.194 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 move easily process.
C. Change the workflow to use amazon kinesis data firehouse to gain a higher throughput.
D. Run the update shardCount command to increase the number of shards in the stream.
Answer: D

NO.195 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.
Answer: B
Explanation
https://aws.amazon.com/rds/ha/

NO.196 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 1AM access and secret key, and store it in the Lambda function.
B. Create an 1AM role to the Lambda function with permissions to list all Amazon RDS instances.
C. Create an 1AM role to Amazon RDS with permissions to list all Amazon RDS instances.
D. Create an 1AM access and secret key, and store it in an encrypted RDS database.
Answer: B
Explanation
https://docs.aws.amazon.com/lambda/latest/dg/vpc-rds.html

NO.197 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 first 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.

Answer: C

NO.198 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

Answer: C

Explanation
Predictive Scaling, a feature of AWS Auto Scaling uses machine learning to schedule the right number of EC2 instances in anticipation of approaching traffic changes. Predictive Scaling predicts future traffic, including regularly-occurring spikes, and provisions the right number of EC2 instances in advance

NO.199 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 Multi-AZ 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

Answer: D

Explanation

https://aws.amazon.com/dms/?nc1=h_ls

NO.200 A company is launching a new static website on Amazon S3 and Amazon CloudFront. The company wants to ensure that all request go thought only Cloud front.

How Can a Solution Architect meet this requirement?

A. Configure the S3 bucket policy to Cloud Front IP address to read object.

B. Create IAM user in a group that the read access to the S3 bucket Configure Cloud Front to pass credentials to the S3 bucket.

C. Create Cloud Front origin access identity (OAI), then update the S3 bucket policy to allow the OAI read access.

D. Convert the S3 bucket to an EC2 instance, then give Cloud Front access to the instance by using security groups.

Answer: C

Explanation

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3 To restrict access to content that you serve from Amazon S3 buckets, you create CloudFront signed URLs or signed cookies to limit access to files in your Amazon S3 bucket, and then you create a special CloudFront user called an origin access identity (OAI) and associate it with your distribution. Then you configure permissions so that CloudFront can use the OAI to access and serve files to your users, but users can't use a direct URL to the S3 bucket to access a file there. Taking these steps help you maintain secure access to the files that you serve through CloudFront.

NO.201 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 S3c

Answer: A

Explanation

your Amazon Aurora storage will automatically grow, up to 64 TB

https://aws.amazon.com/rds/aurora/faqs/

NO.202 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
Answer: A

NO.203 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 Infrequent Access.
Answer: C
Explanation
https://aws.amazon.com/blogs/aws/archive-s3-to-glacier/

NO.204 A company has a requirement to control traffic entering and exiting subnets within its VPC. This includes the ability to explicitly allow or deny certain types of traffic.
This can be accomplished by implementing:
A. security groups
B. network ACLs.
C. route tables
D. virtual private gateways.
Answer: B
Explanation
https://aws.amazon.com/answers/networking/vpc-security-capabilities/
Network ACL
A network access control list (ACL) is an optional layer of security that provides a stateless firewall for controlling traffic in and out of a subnet. Network ACLs support up to 20 IP CIDR-based allow or deny rules for both inbound and outbound traffic. AWS customers typically leverage security groups as their primary method of network packet filtering since they are more versatile than network ACLs due to their ability to perform stateful packet filtering and utilize rules that reference other security groups. However, network ACLs can be effective as a secondary control for denying a specific subset of traffic or providing high-level guard rails for a subnet. By implementing both network ACLs and security groups as a defense-in-depth means of controlling traffic, a mistake in the configuration of

one of these controls will not expose the host to unwanted traffic.

NO.205 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
Answer: C
Explanation
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.h

NO.206 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.
Answer: C
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

NO.207 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
Answer: D
Explanation
"use multivalue answer routing when you want to associate your routing records with a Route 53 health check"
https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/

NO.208 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 1AM policies to require MFA for all users.
C. Federate 1AM against corporate AD that requires MFA.
D. Use Amazon API Gateway and require SSE for photos
Answer: A

NO.209 A Solutions Architect is designing an application on AWS that will connect to the onpremise 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
Answer: B
Explanation
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination. Refer:
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

NO.210 A customer has a legacy application with a large amount of data the files accessed by the application are approximately 10 GB each, but are rarely accessed. However when files are accessed they are retrieved sequentially The customer is migrating the application to AWS and would like to use Amazon EC2 and Amazon EBS What is the LEAST expensive EBS volume type for this use case?
A. Cold HDD (sc1)
B. Provisioned IOPS SSD (io1)
C. General Purpose SSD (gp2)
D. Throughput Optimized HDD (st1)
Answer: A

NO.211 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 reduces 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.
Answer: B
Explanation
https://aws.amazon.com/efs/

NO.212 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.
Answer: A
Explanation
This guidance supersedes any previous guidance on optimizing performance for Amazon S3. https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html For example, previously Amazon S3 performance guidelines recommended randomizing prefix naming with hashed characters to optimize performance for frequent data retrievals. You no longer have to randomize prefix naming for performance, and can use sequential date-based naming for your prefixes

NO.213 A company is designing a website that will be hosted on Amazon S3.
How should users be prevented from linking directly to the assets in the S3 bucket?
A. Create a static website, then update the bucket policy to require users to access the resources with the static website URL.
B. Create an Amazon CloudFront distribution with an Origin Access Identity (OAI) and update the bucket policy to grant permission to the OAI only.
C. Create a static website, then configure an Amazon Route 53 record set with an alias pointing to the static website. Provide this URL to users.
D. Create an Amazon CloudFront distribution with an AWS WAF web ACL that permits access to the origin server through the distribution only.
Answer: B

NO.214 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.
D. Enable the CloudFront option to restrict viewer access and update the bucket policy to allow the distribution.
Answer: B
Explanation
create a CloudFront origin access identity to restrict access to your Amazon S3 content, and grant the origin access identity the desired permissions.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-

restricting-access-to-s3

NO.215 A solutions architect is designing a solution that must store and retrieve session data and JSON documents.
The solution must provide high availability, strong consistency, and data durability Which solution meets these requirements?
A. Amazon DynamoDB table
B. Amazon EBS volume with provisional IOPS
C. AmazonEC2 Instance Tore
D. Amazon SQS
Answer: A

NO.216 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
Answer: B
Explanation
Whenever you see a question that says "data retrieval must occur with minimal latency" and you see S3 and DynamoDB in the options, always choose DynamoDB (9 out of 10 times). There is nothing in this question that points to S3 as the solution but if you still have doubts check the AWS Certification Exam Practice Question in the link below that says "A meteorological system monitors 600 temperature gauges, obtaining temperature samples every minute and saving each sample to a DynamoDB table".
http://jayendrapatil.com/tag/dynamodb/

NO.217 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.
Answer: C

NO.218 An application consists of microservices. The microservices need to communicate asynchronously and the solution must ensure that each message is consumed only once.
Which service should be used?
A. Amazon SQS

B. Amazon Kinesis
C. Amazon SNS
D. AWS STS
Answer: B

NO.219 A Solution Architect is building an application that will run for eight hours, Monday through Friday. This application will also run a weekly batch process every Saturday night that consistently takes four hours to complete.
Which is the MOST cost- effective computer solution?
A. Spot Instances
B. Standard Reserved Instances
C. On-Demand Instances
D. Scheduled Reserved Instances
Answer: D

NO.220 A company has a web application with an apache front end, a Memcached cache, and a postgreSQL database.
The company also has a data warehouse that is accessed with standard SQL tools. The company would like to migrate the architecture to AWS with as little work as possible.
Which of the following AWS services should a solution Architect recommend?
A. Amazon ElastiCache and Amazon Redshift
B. AWS identity and Access Management (1AM) with AWS Lambda
C. Amazon ElastiCache with Redis
D. Amazon DynamoDB end Amazon ElastiCache
Answer: D

NO.221 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)
Answer: A
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

NO.222 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
Answer: C
Explanation
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html

NO.223 A Company wants to organize the contents of multiple websites in managed file storage. The company must be able to scale the storage based on demand without needing to provision storage. Multiple servers should be able to access this storage concurrently.
Which service should the solutions architect recommend?
A. Amazon S3
B. Amazon EBS
C. Amazon EFS
D. AWS Storage Gateway - volume gateway
Answer: C

NO.224 A company provides Amazon S3 access to a small group of users from the Accounting department for a single S3 bucket. A Solutions Architect wants to ensure that users are able to recover data if it was deleted.
Which of the following solutions will helps ensure that data can be easily restored by the Accounting team?
A. Add a bucket policy that requires MFA Delete.
B. Set up an S3 event trigger in AWS Lambda to copy the file to a separate S3 bucket
C. Enable versioning for the S3 bucket
D. Configure an S3 lifecycle rule to transition the Item to another read-only bucket
Answer: C

NO.225 A solutions Architect needs to build a resilient data warehouses using amazon Rehshift. The architect needs to rebuild the Redshift cluster in another region.
Which approach can architect take to address this requirement?
A. Modify the Redshift. cluster and configure cross-region snapshots to the other region
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
Answer: B

NO.226 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.

Answer: D

Explanation

https://aws.amazon.com/about-aws/whats-new/2019/10/amazon-redshift-improves-performance-of-inter-region-s

NO.227 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 fulfill 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

Answer: C

Explanation

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

NO.228 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.

Answer: C

Explanation

Lambda has concurrent limit of 3000 but the question says 10000 for which Docker with Amazon ECS is capable of https://docs.aws.amazon.com/lambda/latest/dg/scaling.html

NO.229 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)

Answer: C

Explanation

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

NO.230 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.
Answer: C

NO.231 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.
Answer: B
Explanation
https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

NO.232 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
Answer: A

NO.233 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.
Answer: C
Explanation

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

NO.234 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

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

Answer: A

NO.235 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 first 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.

Answer: B

Explanation
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html With the default termination policy, the behavior of the Auto Scaling group is as follows: Determine which Availability Zone(s) have the most instances, and at least one instance that is not protected from scale in. If there are multiple unprotected instances to choose from in the Availability Zone(s) with the most instances, an instance is selected for termination based on the following criteria (applied in the order shown).

NO.236 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

Answer: B

Explanation
data stored in Glacier is immutable by default (without any extra adjustments) but for S3 data will be immutable you have to apply S3 Object Lock protection but option A only says S3. Data stored in S3 is not immutable by default without applying object lock protection.

https://aws.amazon.com/glacier/features/

NO.237 A Company will run different data analytics jobs on large petabyte-scale datasets, Using standard SQL and existing business intelligence tools. The data is mostly structured, but part of the data unstructured and resides in Amazon S3.
What Technologies should be used to support this use case?
A. An amazon aurora database cluster with 15 replicas distributed across availability zones.
B. Amazon Redshift with Amazon Redshift Spectrum.
C. Amazon DynamoDB with Amazon DynamoDB Accelerator.
D. Amazon ElastiCache for Redus with cluster mode Enabled.
Answer: B

NO.238 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
Answer: B

NO.239 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.
Answer: A
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

NO.240 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.
Answer: C
Explanation
"Configure the trigger to only apply to a prefix used for incoming objects" should address the concern

with infinite loop when writing back object to same bucket . reference :
https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html

NO.241 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 1AM authorization and add least-privileged permissions to each respective 1AM 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.
Answer: B
Explanation
https://aws.amazon.com/blogs/compute/introducing-custom-authorizers-in-amazon-api-gateway/
Today Amazon API Gateway is launching custom request authorizers. With custom request authorizers, developers can authorize their APIs using bearer token authorization strategies, such as OAuth using an AWS Lambda function. For each incoming request, API Gateway verifies whether a custom authorizer is configured, and if so, API Gateway calls the Lambda function with the authorization token. You can use Lambda to implement various authorization strategies (e.g., JWT verification, OAuth provider callout).
Custom authorizers must return AWS Identity and Access Management (IAM) policies. These policies are used to authorize the request. If the policy returned by the authorizer is valid, API Gateway caches the returned policy associated with the incoming token for up to 1 hour so that your Lambda function doesn't need to be invoked again.

NO.242 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
Answer: D
Explanation
https://aws.amazon.com/cloudhsm/

NO.243 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
Answer: C
Explanation
https://docs.aws.amazon.com/lambda/latest/dg/limits.html

NO.244 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 1TB of data stored.
What type of storage should be used?
A. Amazon S3
B. Amazon EBS
C. Amazon Glacier
D. Amazon EFS
Answer: C
Explanation
https://aws.amazon.com/s3/faqs/?nc=sn&loc=7

NO.245 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
Answer: C

NO.246 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.
Answer: C
Explanation
https://aws.amazon.com/blogs/aws/new-amazon-s3-server-side-encryption/
https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetBucketEncryption.html?shortFooter=true
https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryptionCustomerKeys.html

NO.247 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.
Answer: B

NO.248 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
Answer: A C
Explanation
Amazon SNS works closely with Amazon Simple Queue Service (Amazon SQS). Both services provide different benefits for developers. Amazon SNS allows applications to send time-critical messages to multiple subscribers through a "push" mechanism, which eliminates the need to periodically check or "poll" for updates. Amazon SQS is a message queue service used by distributed applications to exchange messages through a polling model and can be used to decouple sending and receiving components without requiring each component to be concurrently available. By using Amazon SNS and Amazon SQS together, messages can be delivered to applications that require immediate notification of an event and also persisted in an Amazon SQS queue for other applications to process at a later time.

NO.249 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
Answer: D
Explanation
API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. API Gateway has no minimum fees or startup costs. You pay only for

the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales. Aws Lambda: Case study highlights"from several hours to just over 10 seconds, and reduced infrastructure and operational costs." Most gaming website using Lambda.
https://aws.amazon.com/lambda/resources/customer-case-studies/
https://aws.amazon.com/blogs/gametech/game-developers-guide-to-the-aws-sdk/

NO.250 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
Answer: B

NO.251 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.
Answer: C
Explanation
https://aws.amazon.com/blogs/aws/new-host-based-routing-support-for-aws-application-load-balancers/

NO.252 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
Answer: A
Explanation
https://aws.amazon.com/blogs/database/how-to-determine-if-amazon-dynamodb-is-appropriate-for-your-needs-a

NO.253 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
Answer: C
Explanation
"AWS Elastic Beanstalk is the fastest and simplest way to get web applications up and running on AWS.
Developers simply upload their application code and the service automatically handles all the details such as resource provisioning, load balancing, auto-scaling, and monitoring. Elastic Beanstalk is ideal if you have a PHP, Java, Python, Ruby, Node.js, .NET, Go, or Docker web application. Elastic Beanstalk uses core AWS services such as Amazon EC2, Amazon Elastic Container Service (Amazon ECS), Auto Scaling, and Elastic Load Balancing to easily support applications that need to scale to serve millions of users."
https://aws.amazon.com/elasticbeanstalk/details/

NO.254 A solutions Architect is designing a multicontainer-based web application. Parts of the web application,
/orders and /sale-event, must scale independently while maintaining a single fully qualified domain name.
Which AWS services will help the Architect build this platform? (select TWO)
A. Amazon ELB Application Load balancer
B. Amazon ELB classic load balancer
C. AmazonEC2 Container Service
D. Amazon Dyanamo DB
E. Amazon SQS
Answer: A C

NO.255 An organization stores customer files and must frequently increase the size of its on-premises storage system to enable quick access and archiving. The organization needs an AWS solution.
How can this requirement be met at the lowest cost?
A. Use Amazon Glacier for regular storage and Amazon S3 for archiving data.
B. Use Amazon S3 for regular storage and Amazon Glacier for archiving data.
C. Use Amazon EBS for regular storage and Amazon S3 for archiving data.
D. Use Amazon EBS for archiving data and Amazon Glacier for regular storage.
Answer: B

NO.256 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
Answer: A
Explanation
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html

NO.257 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
Answer: C E
Explanation
https://docs.aws.amazon.com/en_pv/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

NO.258 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
Answer: B
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serving-outdated-content-s3/

NO.259 A website keeps a record of user actions using a globally unique identifier (GUID) retrieve from Amazon Aurora in place of the user name within the audit record security protocols state that the GUID state that the GUID content must not leave the company's VPN.
As the web traffic has increase, the number of web servers and azure read replicas has also increased to keep up with the user record for the GUID.
What should be done to reduce the number of read replicas required while improving performance?
A. Keep the user name and GUID in memory on the web server instance so that the association can be remade on demand Remove the record after 30 minutes
B. Deploy a Amazon ElastiCache for Redis server into the infrastructure and store the user name and GUID there Retrieve the GUID from ElastiCache when required
C. Encrypt the GUID using Base64 and store it in the users session cookie Decrypt the GUID when an audit record is needed
D. Change the GUID to an MD5 hash of the user name, so that the value can be calculated on

demand without referring to the database

Answer: B

Explanation

https://www.lleicloud.com/index.php/aws-certified-solutions-architect-associate-c01-2019-7/

NO.260 An application stores data in a My SQL database hosted on an EC2 instance. A Solutions Architect must address reports of high latency and dropped requests. The web tier EC2 instances are mostly idle, but the database instance has a large number of read requests that result in a large-disk read queue.

Which solution will address the problems?

A. Provision all the EC2 instances, both web tier and database, in a placement group.

B. Provision a database replica, and place a Network Load Balancer in front of both databases.

C. Import the database into a Mufti-AZ RDS instance and direct the read-only queries to the standby instance.

D. Cache database query results in an Amazon ElastiCache cluster, and check the cluster for cached results before calling the database.

Answer: D

NO.261 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.

Answer: A

Explanation

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

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

NO.262 A company with an existing AWS VPC is experiencing an increasing number of malicious attacks from a particular IP address range. The company wants to block all access from these IP addresses while the abuse patterns are being investigated.

How can access from the specified IPs be denied quickly and temporarily?

A. Use an AWS Marketplace solution to block access from the specified IP range.

B. Leverage NAT gateway on each instance to block access from the specified IP range.

C. Use network ACLs to block access from the specified IP range.

D. Create a rule in the security groups to block access from the specified IP range.

Answer: C

NO.263 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.

Answer: C

NO.264 A retail company runs hourly flash sales and has a performance issue on its Amazon RDS for PostgreSQL database. The Database Administrators have identified that the issue with performance happens when finance and marketing employees refresh sales dashboards that are used for reporting real-time sales data.

What should be done to resolve the issue without impacting performance?

A. Create a Read Replica of the RDS PostgroSQL database and point Hie dashboards at the Read Replica

B. Move data from tie RDS PostgreSQL database to Amazon Redshift nightly and point the dashboards at Amazon Redshilt

C. Monitor the database with Amazon CloudWatch and increase the instance $126 as necessary Make no changes to the dashboards

D. Take an hourly snapshot of the RDS PostgreSQL database and load the hourly snapshots to another database to which the dashboards in pointed

Answer: A

NO.265 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.

Answer: A

Explanation

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

NO.266 A Solutions Architect is reviewing an application that writes data to an Amazon DynamoDB table on a daily basis. Random table reads occur many times per second. The company needs to allow thousands of low-latency reads and avoid any negative impact to the rest of the application

What should the Solutions Architect do to meets the company's goals?

A. Use DynamoDB Accelerator to cache reads

B. Increase DynamoDB write capacity units
C. Add Amazon SQS to decouple requests
D. Implement Amazon Kinesis to decouple requests
Answer: A
Explanation
https://aws.amazon.com/dynamodb/dax/
"Extreme Performance
While DynamoDB offers consistent single-digit millisecond latency, DynamoDB + DAX takes performance to the next level with response times in microseconds for millions of requests per second for read-heavy workloads. With DAX, your applications remain fast and responsive, even when a popular event or news story drives unprecedented request volumes your way. No tuning required. "

NO.267 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 1AM 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.
Answer: D
Explanation
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-create-queue.html#crea

NO.268 A Solutions Architect is designing a ride-sharing application. The application needs consistent and single-digit millisecond latency. In addition, the application must integrate with a highly scalable and fully managed database service to track GPS coordinates and user data for all rides.
Which database service should the Solutions Architect use to meet these performance requirements ?
A. Amazon RDS
B. Amazon Redshift.
C. Amazon DynamoDB.
D. Amazon Aurora.
Answer: C
Explanation
https://aws.amazon.com/dynamodb/

NO.269 A solutions architect needs to convert potential single points of failure to a highly-available configuration. The currently architecture contains amazon EC2 instances with databases running in one availability zone.
Web-tier resources have not been given public addresses, but still require internet access.
Which solution should the architect use to maintain high availability?

A. Use ELB Classic Load Balancer with the web tier Deploy EC2 instances in two Availability Zones and enable Multi-AZ RDS Deploy a NAT gateway in one Availability Zone
B. Use ELB Classic Load Balancer with the web tier Deploy EC2 instances in two Availability Zones and enable Multi-AZ RDS Deploy NAT gateways in both Availability Zones
C. Use ELB Classic Load Balancer with the database tier Deploy Amazon EC2 instances in two Availability Zones and enable Multi-AZ RDS Deploy NAT gateways in both Availability Zones
D. Use ELB Classic Load Balancer with the database tier Deploy Amazon EC2 instances in two Available Zones and enable Multi-AZ RDS Deploy a NAT gateway in one Availability Zone
Answer: B
Explanation
"If you have EC2 instances in multiple Availability Zones and these share one NAT gateway, in the event of AZ failure the NAT gateway becomes unavailable and the resources within other Availability Zones lose internet access. To create a fault-tolerant architecture, make sure that your AWS NAT gateways are deployed in at least two Availability Zones (AZs)"

NO.270 A Solutions Architect is designing the infrastructure for web application. One of the requirements is to notify an administrator by email of new registrations. Simultaneously, the user's email address must be sent to a Lambda function that will perform additional user verification.
Which of the following services meet the specified requirements while minimizing architectural complexity?
A. Amazon SNS
B. Amazon Kinesis
C. AWS ClotioTrail
D. Amazon SQS
Answer: D

NO.271 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 fit 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.
Answer: B
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

NO.272 A customer is deploying a production portal application on AWS. The database tier has structured data. The company requires a solution that is easily manageable and highly available.
How can these requirements be met?
A. Deploy the database on multiple Amazon EC2 instances backed by Amazon EBS across multiple Availability Zones.
B. Use Amazon RDS with a multiple Availability Zone option.
C. Use RDS with a single Availability Zone option and schedule periodic database snapshots.

D. Use Amazon DynamoDB.

Answer: B

Explanation

https://aws.amazon.com/rds/

NO.273 A Solution Architect works for an insurance company that has a large number of patient health records. Each record will be used once when assessing a patient and will need to be securely stored for seven years to meet regulations. In rare cases the Solution Architect may need to retrieve a patient record in five hours.

Which type of AWS storage would deliver the most cost-effective solution?

A. Amazon S3 Reduced Redundancy Storage

B. Amazon S3

C. Amazon Glacier

D. Amazon S3 Infrequent Access

Answer: C

NO.274 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)

Answer: A

Explanation

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#:~:targetText=Instance%20store

NO.275 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

Answer: D

NO.276 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)

Answer: C

Explanation

SSE-S3: AWS manages both data key and master key

SSE-KMS: AWS manages data key and you manage master key

SSE-C: You manage both data key and master key

NO.277 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

Answer: C

NO.278 A Solutions Architect is planning a new web application in an Amazon VPC. The customer has specified that the architecture for the new web application must include the capability of sharing session state among a highly available group of web servers.

To fulfill this requirement, the Solutions Architect should:

A. deliver session stale as messages in the Amazon SOS queue

B. enable session state on Amazon CloudFront

C. store session state in Amazon ElastiCache

D. provide session state through Elastic Load Balancing sticky sessions

Answer: D

NO.279 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

Answer: B

NO.280 A customer needs to capture all client connection information from their load balancer every five minutes. The company wants to use data for analyzing traffic patterns and troubleshooting

their applications. Which of the following options meets the customer requirements?

A. Enable access logs on the Application load balancer

B. Enable AWS CloudTrail for the Application load balancer

C. Enable Amazon CloudWatch metrics on the Application load balancer

D. Install the Amazon CloudWatch Logs agent on the Application load balancer

Answer: A

NO.281 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.

Answer: B

Explanation

AWS PrivateLink simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet. AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network.

https://aws.amazon.com/privatelink/

NO.282 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

Answer: B

NO.283 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.
Answer: B
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/requesting-ebs-volume-modifications.html
Requesting Modifications to Your EBS Volumes With Elastic Volumes, you can dynamically modify the size, performance, and volume type of your Amazon EBS volumes without detaching them. Use the following process when modifying a volume: (Optional) Before modifying a volume that contains valuable data, it is a best practice to create a snapshot of the volume in case you need to roll back your changes. For more information, see Creating Amazon EBS Snapshots. Request the volume modification. Monitor the progress of the volume modification. For more information, see Monitoring the Progress of Volume Modifications. If the size of the volume was modified, extend the volume's file system to take advantage of the increased storage capacity. For more information, see Extending a Linux File System After Resizing a Volume.

NO.284 A company's website receives 50,000 requests each second, and the company wants to use multiple applications to analyze 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
Answer: A
Explanation
https://aws.amazon.com/blogs/big-data/create-real-time-clickstream-sessions-and-run-analytics-with-amazon-kin

NO.285 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
Answer: D

Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html

NO.286 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
Answer: A

NO.287 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.
Answer: B
Explanation
https://aws.amazon.com/blogs/aws/protect-your-data-with-new-ebs-encryption/

NO.288 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
Answer: D
Explanation
https://www.sumologic.com/blog/kinesis-streams-vs-firehose/
Check out the 'key concepts' section:
"Shards scale linearly, so adding shards to a stream will add 1MB per second of ingestion, and emit data at a rate of 2MB per second for every shard added. Ten shards will scale a stream to handle 10MB (10,000 PUTs) of ingress, and 20MB of data egress per second"

NO.289 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 taked 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.
Answer: A

NO.290 A company will host a static website within an Amazon S3 bucket. The website will serve millions of users globally, and the company wants to minimize data transfer costs.
What should the Solutions Architect do to ensure costs are kept to a minimum?
A. implement an AWS Auto Scaling group for the website to ensure grows with use.
B. Use cross-region replication to copy the website to an additional S3 bucket in a different region
C. Create an Amazon CloudFront distribution, with the S3 bucket as the origin server
D. Move the website to large compute-optimized Amazon EC2 instances
Answer: C

NO.291 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
Answer: B
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

NO.292 Servers in the VPC require internet access for system patching. A solutions Architect needs to enable Internet access to the servers, while ensuring that the servers are not exposed to the internet.
What should the Architect use to meet this requirement?
A. Virtual Private Gateway
B. NAT Gateway
C. ELB Classic Load Balancer
D. Amazon CloudFront
Answer: B

NO.293 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

Answer: B

Explanation

https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/ Use encryption to protect your data If your use case requires encryption during transmission, Amazon S3 supports the HTTPS protocol, which encrypts data in transit to and from Amazon S3. All AWS SDKs and AWS tools use HTTPS by default.

Note: If you use third-party tools to interact with Amazon S3, contact the developers to confirm if their tools also support the HTTPS protocol.

NO.294 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.

Answer: D

Explanation

Amazon S3 offers eventual consistency for overwrite PUTS and DELETES in all Regions. Updates to a single key are atomic. For example, if you PUT to an existing key, a subsequent read might return the old data or the updated data, but it never returns corrupted or partial data. Amazon S3 achieves high availability by replicating data across multiple servers within AWS data centers. If a PUT request is successful, your data is safely stored. However, information about the changes must replicate across Amazon S3, which can take some time, and so you might observe the following behaviors: A process writes a new object to Amazon S3 and immediately lists keys within its bucket. Until the change is fully propagated, the object might not appear in the list.

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

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

NO.295 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-1 a, sa-east-1 b, and sa-east-1 c.

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-1 a, six Amazon EC2 instances in saeast-1 b, and six Amazon EC2 instances in sa-east-1 c

B. Deploy six Amazon EC2 instances in sa-east-1 a, four Amazon EC2 instances in saeast-1 b, and two Amazon EC2 instances in sa-east-1 c

C. Deploy three Amazon EC2 instances in sa-east-1 a, three Amazon EC2 instances in sa-east-1 b, and three Amazon EC2 instances in sa-east-1 c

D. Deploy two Amazon EC2 instances in sa-east-1 a, two Amazon EC2 instances in saeast-1 b, and two

Amazon EC2 instances in sa-east-1 c
Answer: C

NO.296 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.
Answer: D
Explanation
https://aws.amazon.com/blogs/developer/accessing-private-content-in-amazon-cloudfront/

NO.297 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.
Answer: A D
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

NO.298 Which of the following techniques should an Amazon DynamoDB customer follow the maximize throughput?
A. Create tables with as few partition keys as possible.
B. Create tables with a partition key that has a large number of distinct values requested uniformly.
C. Create tables with a partition key that has a small number of distinct values requested uniformly.
D. Create tables with only range keys.
Answer: B

NO.299 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 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.
Answer: D

NO.300 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. Reduced Redundancy Class (RRS)
Answer: C
Explanation
https://aws.amazon.com/s3/storage-classes/

NO.301 A company has two different types of reporting needs on their 200-GB data warehouse:
1 Data scientists run a small number of concurrent ad hoc SQL queries that can take several minutes each to run.
2 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.
Answer: C
Explanation
Redshift makes it simple and cost effective to run high performance queries on petabytes of structured data so that you can build powerful reports and dashboards using your existing business intelligence tools.
https://docs.aws.amazon.com/redshift/latest/dg/c_workload_mngmt_classification.html

NO.302 A company processes mobile chat messages. Throughput can increase dramatically, and the Amazon EC2 infrastructure cannot handle the fluctuating demand. Messages are received in an Amazon Kinesis Data Stream, and the processor instances are deployed in an Auto Scaling group. A

CloudWatch alarm, which uses Amazon SNS to tiger a Lambda function, automatically scales the Kinesis Data Stream. The processor instances' application code and configuration are stored in an S3 bucket.

A. How can a Solution Architect improve the launch time of new instances in the Auto Scaling group?

B. Reduce the values of the Default Cooldown and Health Check Grace Period settings for the Auto Scaling group.

C. Change the scale-out rules for the Auto Scaling group to launch instances at a lower threshold on the Kinesis CloudWatch alarm.

D. Modify the Lambda function to change the number of Auto Scaling group members when it updates the Kinesis Shard count.

E. Update the launch configuration to use a custom Amazon Machine Image (AMI) with all the software pre-installed. Use user data scripts to pull the configuration at launch from Amazon S3.

Answer: A

NO.303 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

Answer: C

NO.304 Which Service would you 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 Pipelineweb

Answer: B

NO.305 A company is developing an application to deliver dynamic content to users the globe. The content should to customize according to a user's device and be delivered with very low latency.

Which service should be used?

A. Amazon API Gateway

B. Amazon Cloud Front

C. Amazon S3

D. Lamba@Edge

Answer: B

Explanation

https://aws.amazon.com/cloudfront/dynamic-content/

NO.306 The application tier for a workload runs on EC2 instances that are unevenly distributed across two Availability Zones. The instances are behind a Network Load Balancer and are accessed through layer 4 TCP connections.
The instances in the lesser populated Availability Zone are failing as the result of high CPU utilization.
Which configuration change can help mitigate the issue?
A. Modify the Network Load Balancer to enable sticky sessions
B. Modify the Network Load Balancer to enable cross-zone load balancing.
C. Switch to using an Application Load Balancer and enable sticky sessions.
D. Switch to using an Application Load Balancer and enable cross-zone load balancing.
Answer: D

NO.307 Which tool analyzes account resources and provides a detailed inventory of changes over time?
A. AWS Config
B. AWS CloudFormation
C. Amazon CloudWatch
D. AWS Service Catalog
Answer: A
Explanation
https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html

NO.308 An application runs on Amazon EC2 instances in an Auto Scaling group. When instances are terminated, the Systems Operations team cannot determine the route cause, because the logs reside on the terminated instances and 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.
Answer: C
Explanation
https://aws.amazon.com/blogs/aws/cloudwatch-log-service/

NO.309 A company has thousands of files stored in an Amazon S3 bucket that has a welldefined access pattern. The files are accessed by an application multiple times a day for the first 30 days. Files are rarely accessed within the next 90 days. After that, the files are never accessed again. During the first 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 first 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 first 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 first 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 first 30 days. After that, move the data to the GLACIER storage class, where is will be deleted automatically.

Answer: B

NO.310 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

Answer: C

Explanation

https://www.cirrusup.cloud/s3-vs-dynamodb-price-comparison/

NO.311 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

Answer: D

Explanation

Elasticache (Redis and Memcached) is an in-memory cache for RDS DB instances and it helps improve performance by diverting frequently accessed read queries to the elasticache.

NO.312 A company needs to capture all client connection information from its Application Load Balancer every five minutes. This data will be used to analyze 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

Answer: B

NO.313 An application has components running in a public subnet and a private subnet. The components within the private sub net must connect to the internet to receive updates.

How should this be accomplished without moving the components into a public subnet?

A. Add an internet gateway to the private subnet and update the private subnet route table.

B. Add a NAT gateway to the public subnet and update the public subnet route table.
C. Add an internet gateway to the VPC and update the private subnet route table.
D. Add a NAT gateway to the public subnet and update the private subnet route table.
Answer: D
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

NO.314 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 analyzed 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 FIDD volumes.
Answer: A
Explanation
What Is Amazon Kinesis Data Firehose?
Amazon Kinesis Data Firehose is a fully managed service for delivering real-time streaming data to destinations such as Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Elasticsearch Service (Amazon ES), and Splunk. Kinesis Data Firehose is part of the Kinesis streaming data platform, along with Kinesis Data Streams, Kinesis Video Streams, and Amazon Kinesis Data Analytics. With Kinesis Data Firehose, you don't need to write applications or manage resources. You configure your data producers to send data to Kinesis Data Firehose, and it automatically delivers the data to the destination that you specified. You can also configure Kinesis Data Firehose to transform your data before delivering it

NO.315 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
Answer: A

NO.316 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.
Answer: C

NO.317 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
Answer: B

NO.318 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.
Answer: C
Explanation
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html

NO.319 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.
Answer: B
Explanation
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html

NO.320 A company plans to use Amazon GuardDuty to detect unexpected and potentially malicious activity. The company wants to use Amazon CloudWatch to ensure that when findings occur, remediation takes place automatically.
Which CloudWatch feature should be used to trigger an AWS Lambda function to perform the remediation?
A. Events
B. Dashboards
C. Metrics
D. Alarms
Answer: A
Explanation
https://aws.amazon.com/guardduty/

NO.321 An application runs on Amazon EC2 instances in multiple Availability Zones (AZs) behind an Application Load Balancer. The load balancer is in public subnets; the EC2 instances are in private subnets and must not be accessible from the internet. The EC2 instances must call external services on the internet. If one AZ becomes unavailable, the remaining EC2 instances must still be able to call the external services.
How should these requirements be met?
A. Create a NAT gateway attached to the VPC. Add a route to the gateway to each private subnet route table.
B. Configure an internet gateway. Add a route to the gateway to each private subnet route table.
C. Create a NAT instance in the private subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT instance.
D. Create a NAT gateway in each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT gateway.
Answer: D
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
If you have resources in multiple Availability Zones and they share one NAT gateway, in the event that the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone. "

NO.322 A customer notices that their Amazon S3 bucket is experiencing elevated GET requests after a recent marketing campaign. The Amazon S3 request pricing is now too expensive.
What solutions would help reduce their costs?

A. Configure the Amazon S3 bucket to cross region replicate their data to an Amazon ElasticacheRedis cluster
B. Place Amazon cloudfront in front of the Amazon S3 bucket and enable caching for the content being requested.
C. Use Amazon Cloudwatch to monitor the GET request metrics and disable the Amazon S3 bucket when the request count breaches a specified threshold
D. Create an Amazon EC2 Auto Scaling group that host web servers that make requests to the Amazon S3 bucket and place an elastic load balancer in front of the instances.
Answer: B

NO.323 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.
Answer: A
Explanation
https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html

NO.324 A company wants to store data on AmazonS3 and requires a solution that can recover from accidental deletion of data. What is the MOST simple and cost-effective solution to accomplish this goal?
A. Create two S3 buckets and use a scheduled job using AmazonS3 CLI to replicate data between buckets.
B. Create two S3 buckets in different regions and enable cross-region replication between buckets.
C. Create a new bucket and enable bucket versioning from AWS Management console
D. Create a new bucket and trigger a Lambda event on all newly updated objects to copy data to another S3 bucket
Answer: C

NO.325 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 beminimized.
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.
Answer: C
Explanation
To minimize downtime, you can Modify an Amazon RDS instance to a Multi-AZ deployment. For Multi-AZ deployments, OS maintenance is applied to the secondary instance first, then the instance

fails over, and then the primary instance is updated.
https://aws.amazon.com/premiumsupport/knowledge-center/rds-required-maintenance/
https://aws.amazon.com/rds/ha/

NO.326 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

Answer: B
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

NO.327 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 (1AM) policies that enforce the corporate VPC architecture standards

Answer: C
Explanation
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-nested-stacks.html

NO.328 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.

Answer: A D
Explanation
Data lakes built on AWS primarily use two types of encryption: Server-side encryption (SSE) and client-side encryption. SSE provides data-at-rest encryption for data written to Amazon S3. With SSE, Amazon S3 encrypts user data assets at the object level, stores the encrypted objects, and then decrypts them as they are accessed and retrieved. With client-side encryption, data objects are

encrypted before they written into Amazon S3.
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html

NO.329 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
Answer: C

NO.330 A customer 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 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
Answer: B
Explanation
Many companies consider migrating from relational databases like MySQL to Amazon DynamoDB, a fully managed, fast, highly scalable, and flexible NoSQL database service. For example, DynamoDB can increase or decrease capacity based on traffic, in accordance with business needs. The total cost of servicing can be optimized more easily than for the typical media-based RDBMS.
https://aws.amazon.com/blogs/big-data/near-zero-downtime-migration-from-mysql-to-dynamodb/

NO.331 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:
1 Protocol: TCP
2 Port Range: 1433 (MS SQL)
3 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.
Answer: D

NO.332 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
Answer: B
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-fleet.html
https://stackoverflow.com/questions/2312969/webservices-are-stateless
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-fleet-automatic-scaling.html

NO.333 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 I GW.
Answer: B D
Explanation
https://docs.aws.amazon.com/lambda/latest/dg/services-rds-tutorial.html

NO.334 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.
Answer: B
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

NO.335 A company has an application running as a service in Amazon ECS using the Amazon E.C2 launch type. The application code makes AWS API calls to publish messages to Amazon SQS What is the MOST secure method of giving the application permission to publish messages to Amazon SQS?

A. Use AWS IAM to grant SQS permissions to the rote used by the launch configuration tor the Auto Scaling group of the ECS duster

B. Create a new identity and access management (!AM) user with SQS permissions and then update the task definition to declare the access key ID and secret access key as environment variables

C. Create a new identity and access management (1AM) role with SQS permissions and then update the task definition to use this role for the task role setting

D. Update the security group used by the ECS cluster to allow access to Amazon SQS

Answer: A

NO.336 As part of a migration strategy, a Solutions Architect needs to analyze 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 (1AM) 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.

Answer: C
Explanation
https://docs.amazonaws.cn/en_us/cognito/latest/developerguide/what-is-amazon-cognito.html

NO.337 A company with thousands of customers is designing a log-aggregation platform to track customer interactions. The platform will store user interaction data in Amazon S3.
Which of the following strategies will provide improved performance for both data upload and data query?

A. Create a separate bucket in S3 for each customer and use Amazon Athena to query it as needed, to provide maximum flexibility for users

B. Arrange the data in S3 by customer name and date (mybucketcustomer1/YYYY-MM-DD/). so that it can be retrieved in an ordered manner

C. Arrange the data in S3 using a random hash prefix followed by a randomly-generated customer ID (mybucket c34a/a42d113&), and use Amazon CloudFront to access it.

D. Separate each log file as it comes in by date and time using AWS Lambda, and arrange it in S3 according to a timestamp prefix (mybucket/part1/YYYY-MM-DD-hh-mm).

Answer: C

NO.338 A company maintains an application on an on-premises server. The company wants to automatically redirect users to a static maintenance page hosted on Amazon S3 when the application is unavailable.
What is the MOST efficient method to ensure the users are automatically redirected?
A. Use an Amazon Route 53 failover routing policy, and configure the application as primary and the Amazon S3 static page as secondary.
B. Use Amazon CloudWatch Events to trigger an AWS Lambda function that changes the DNS to point to the static page.
C. Use an Amazon Route 53 weighted routing policy, and configure the application higher and the Amazon S3 static page lower.
D. Use Amazon Route 53 to set up multiple A records for both the application and Amazon S3.
Answer: A

NO.339 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-southeast-2.
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.
Answer: D
Explanation
You can also enable MFA delete capability for versioning, which provides an additional layer of security so that you have to provide an MFA token or security code to delete an object inside a bucket. Using cross-region replication requires versioning enabled on the source bucket as well as the destination bucket.

NO.340 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.
Answer: B

NO.341 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 Ute 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
D. Amazon S3 Standard
Answer: B

NO.342 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
Answer: D
Explanation
https://aws.amazon.com/s3/faqs/

NO.343 A team has developed a new web application in an AWS Region that has three Availability Zones: AZ-a, AZ-b, and AZ-c. This application must be fault tolerant and needs at least six Amazon EC2 instances running at all times. The application must tolerate the loss of connectivity to any single Availability Zone so that the application can continue to run.
Which configurations will meet these requirements? (Select TWO)
A. AZ-a with six EC2 instances, AZ-b with six EC2 instances, and AZ-c with no EC2 instances.
B. AZ-a with four EC2 instances, AZ-b with two EC2 instances, and AZ-c with two EC2 instances.
C. AZ-a with two EC2 instances, AZ-b with two EC2 instances, and AZ-c with two EC2 instances.
D. AZ-a with three EC2 instances, AZ-b with three EC2 instances, and AZ-c with no EC2 instances.
E. AZ-a with three EC2 instances, AZ-b with three EC2 instances, and AZ-c with three EC2 instances.
Answer: A E

NO.344 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 1AM 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
Answer: A
Explanation

https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html
"Using CMKs and Data Keys
When you create an encrypted Amazon EBS volume, you specify an AWS KMS customer master key (CMK).
By default, Amazon EBS uses the AWS managed CMK for Amazon EBS in your account. However, you can specify a customer managed CMK."

NO.345 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 twominute 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.
Answer: A
Explanation
https://aws.amazon.com/blogs/compute/taking-advantage-of-amazon-ec2-spot-instance-interruption-notices/

NO.346 A Solutions Architect is designing a process that updates data in a database when any EC2 instance is launched, stopped, or terminated. This update must be performed as close to the EC2 change as possible. The Solutions Architect will use a CloudWatch Event Rule based on EC2 state changes.
Which solution should the Solutions Architect use to achieve this in the MOST cost-effective way?
A. Use an Amazon SQS queue Provision an EC2 instance to poll the queue and update the database
B. Create a Lambda function triggered by Amazon CloudWatch Events to directly update the database
C. Create an Amazon Kinesis Data Stream Launch a Kinesis Data Stream worker to update the database
D. Use an Amazon SQS queue Have a scheduled Lambda function read the queue and update the database.
Answer: B

NO.347 A compliance requirement states that an organization must save documents for 5 years, but the documents must be retrievable within 24 hours of a request.
What is the most cost-effective AWS storage solution?
A. Amazon S3 Standard
B. Amazon S3 Infrequent Access
C. Amazon Glacier

D. Amazon EBS
Answer: B

NO.348 A company wants to analyze 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
Answer: D

NO.349 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.
Answer: A
Explanation
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html

NO.350 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.
Answer: B E
Explanation
Due to the reverse proxy being a bottleneck to scalability, we need to replace it with a solution that can perform content-based routing. This means we must use an ALB not a CLB as ALBs support path-based and host-based routing Auto Scaling should be added to the architecture so that the back end EC2 instances do not become a bottleneck. With Auto Scaling instances can be added and removed from the back end fleet as demand changes A Classic Load Balancer cannot perform content-based routing so cannot be used It is unknown how the reverse proxy can be scaled with Auto Scaling however using an ALB with content-based routing is a much better design as it scales automatically

and is HA by default Burstable performance instances, which are T3 and T2 instances, are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload. CPU performance is not the constraint here and this would not be a cost-effective solution.

NO.351 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 1AM role to the EC2 instance with an 1AM 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.
Answer: D

NO.352 A company has enabled IPv6 in Amazon VPC wants to avoid having resources on the internet initiate communication with instances inside the private subnet. However, these instances need to communicate with the internet.
Which VPC component should the company use?
A. A NAT Gateway
B. An internet gateway
C. A security group
D. An egress-only internet gateway
Answer: A

NO.353 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.
Answer: B

NO.354 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.
Answer: D E
Explanation
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingHostedZone.html
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

NO.355 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
Answer: B

NO.356 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.

Answer: D
Explanation
https://www.cloudberrylab.com/resources/blog/amazon-s3-lifecycle-rules-upload-to-glacier/

NO.357 A Solutions Architect needs to allow developers to have SSH connectivity to web servers. The requirements are as follows:
1 Limit access to users origination from the corporate network.
2 Web servers cannot have SSH access directly from the Internet.
3 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 1AM role to the bastion host with relevant permissions.
D. Configure the web servers' security group to allow SSH traffic from a bastion host.
E. Deny all SSH traffic from the corporate network in the inbound network ACL.
Answer: B D
Explanation
https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/

NO.358 A reporting application running on Amazon EC2 stores data in an Amazon Aurora MySQL cluster that is read-heavy. End-of-month reporting activities put additional heavy read demands on the database. Over the past months, the Operations team has had to increase and decrease the size of the instances in the database cluster several times to accommodate end-of-month reporting demands, incurring downtime in the process.
Management wants to eliminate the downtime but is unwilling to incur the cost of permanently provisioning larger instances.
Which solution meets the requirements with the FEWEST changes to the application code?
A. Use Amazon ElasticCache to implement a query-caching solution
B. Migrate frequently queried data to Amazon DynamoDB to query for reporting
C. Add a read replica to the Amazon Aurora cluster, and use this instance for reporting
D. Create an Auto Scaling policy to add and remove read replicas from the cluster automatically
Answer: C

NO.359 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.
Answer: B

NO.360 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.
Answer: C

NO.361 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.
Answer: C
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service,

NO.362 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.
Answer: C D

Explanation
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html

NO.363 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
Answer: A

NO.364 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
Answer: A
Explanation
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.Endpoints.html
https://developer.rackspace.com/blog/Understanding-Amazon-Aurora-Endpoints/

NO.365 An application is used by thousands of concurrent users. Eighty percent of users access the same content inside the Amazon RDS multi-AZ database.
How can the overall performance of the database queries be improved?
A. Use an Amazon Redshift cluster
B. Use Amazon CloudFront in front of RDS
C. Use Amazon ElastiCache in front of RDS
D. Use Amazon DynamoDB to store the most queried information
Answer: C

NO.366 A Solutions Architect requires a Continuous Integration/Continuous Deployment (CI/CD) pipeline. The pipeline must simultaneously manage and track batches of changes across multiple files. The pipeline must have the ability to deploy applications to Amazon EC2 instances automatically
Use of what Amazon services will meet these requirements?
A. Amazon S3 with object versioning and AWS Elastic Beanstalk
B. AWS CodeCommit and AWS CodeDeploy
C. AWS CodePipeline and Elastic Beanstalk
D. Amazon Elastic File System and CodeDeploy

Answer: C

NO.367 An environment has an Auto Scaling group across two Availability referred to as AZ-a and AZ-b and a default termination policy AZ-a has four Amazon EC2 instances, and AZ-b has three EC2 instances. None of the instances is protected from a scale-in.
How will Auto Scaling proceed if there is a scale-in event?

A. Auto Scaling selects an instance to terminate randomly

B. Auto Scaling terminates the instance with the oldest launch configuration of all instances

C. Auto Scaling selects the Availability Zone with four LC2 instances and then continues to evaluate

D. Auto Scaling terminates the instance with the closest next billing hour ot all instances

Answer: C
Explanation
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html With the default termination policy, the behavior of the Auto Scaling group is as follows:
Default Termination Policy
This section describes the default termination policy used by an Auto Scaling group when a scale-in event occurs. The default termination policy is designed to help ensure that your instances span Availability Zones evenly for high availability. The default policy is kept generic and flexible to cover a range of scenarios.
With the default termination policy, the behavior of the Auto Scaling group is as follows:
1) Determine which Availability Zone(s) have the most instances, and at least one instance that is not protected from scale in.
If there are multiple unprotected instances to choose from in the Availability Zone(s) with the most instances, an instance is selected for termination based on the following criteria (applied in the order shown).

NO.368 An application provides a feature that allows users to securely download private and personal files. The web server is currently overwhelmed with serving files for download. A solutions architect must find a more effective solution to reduce web server load and costs and must allow users to download only their own files.
Which solution meets all requirements?

A. Store the files security on Amazon S3 and have the application generation on Amazon S3 pre-signed URL for the user to download.

B. Store the files in an encrypted Amazon EBS volume, and use a separate set of servers to serve the downloads.

C. Have the application encryption encrypt the files and store them in the local Amazon EC2 instance Store prior to serving them up for download.

D. Create an Amazon CloudFront distribution to distribute and cache the files.

Answer: A
Explanation
https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html

NO.369 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.
Answer: B
Explanation
Built-in auditing AWS KMS is integrated with AWS CloudTrail to record all API requests, including key management actions and usage of your keys.

NO.370 A company had decided to store its critical data on the AWS Cloud. Newly uploaded data is frequently accessed for a period of one month, after which the data is no longer frequently accessed. However, there is a requirement for older objects with a specific prefix to be accessed within milliseconds.
What services and features should the company use to meet this requirement is a durable, available, and cost-effective manner?
A. Use the S3 Standard storage class to store the objects for the initial month. After one month, use lifecycle transition policies to change the storage class for objects with the prefix to S3 STANDARDJA and the rest of the data to Amazon Glacier
B. Use the S3 Standard storage class to store the objects for the initial month. After one month use lifecycle transition policies to change the storage class for all data to Amazon Glacier
C. Use the S3 STANDARDJA storage class to store the objects for the initial month. After one month, use lifecycle transition policies to change the storage class for the objects with the prefix to S3 ONEZONEJA and the rest of the data to Amazon Glacier
D. Use the S3 STANDARDJA storage class to store the objects for the initial month. After one month, use lifecycle transition policies to change the storage class for all data to S3 ONEZONE_IA
Answer: D

NO.371 A company is creating an application that allows users to share uploaded files with other users. They have configured an S3 bucket, where the files are uploaded and stored, to grant access to only an Amazon CloudFront distribution. The company is now asking the solutions Architect to determine a strategy to secure the static files so that they are shared only with the users that the file owner has allowed.
What should the Solutions Architect recommend to secure the static files and prevent unauthorized access?
A. Use the application to create temporary access and secret keys by using AWS STS Assume Role with the policy parameter
B. Use the application instances to create a CloudFront signed URL
C. Use the application instances to create an S3 presigned URL
D. Create a CloudFront origin access identity (OAI) for each user and set the bucket poky for each OAI based on user request
Answer: D

NO.372 A Solutions Architect created an Amazon VPC with two public subnets and two private subnets. A corporate security mandate requires all Amazon EC2 instance be launched in a private

subnet. However, when an EC2 instance running Apache on ports 80 and 443 is launched in the private subnet, no external internet traffic can connect with the server.
What actions should be taken address this situation?

A. Ensure the security group attached to the EC2 instance allows HTTP traffic on port 80 and HTTPS traffic on port 443. Ensure external DNS resolution directs to the IP address of the EC2 instance

B. Launch a NAT Gateway in the private subnet, change the default route to the NAT Gateway, and attach a public Elastic IP address to the NAT Gateway. Ensure external DNS resolution directs to the Elastic IP address

C. Launch an internet-facing Application Load Balancer with the EC2 instance as its endpoint. Ensure external DNS resolution directs to the Application Load Balancer

D. Attach the EC2 instance to an Auto Scaling group in the private subnet. Ensure external DNS resolution directs to the Auto Scaling group

Answer: C

NO.373 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

Answer: D

Explanation
The streaming source for your application. You can select either a Kinesis data stream or a Kinesis Data Firehose data delivery stream as the streaming source. In the input configuration, you map the streaming source to an in-application input stream. The in-application stream is like a continuously updating table upon which you can perform the SELECT and INSERT SQL operations. In your application code, you can create additional in-application streams to store intermediate query results.
Amazon Kinesis Data Analytics is the easiest way to analyze streaming data, gain actionable insights, and respond to your business and customer needs in real time. Amazon Kinesis Data Analytics reduces the complexity of building, managing, and integrating streaming applications with other AWS services. SQL users can easily query streaming data or build entire streaming applications using templates and an interactive SQL editor. Java developers can quickly build sophisticated streaming applications using open source Java libraries and AWS integrations to transform and analyze data in real-time. Amazon Kinesis Data Analytics takes care of everything required to run your real-time applications continuously and scales automatically to match the volume and throughput of your incoming data. With Amazon Kinesis Data Analytics, you only pay for the resources your streaming applications consume. There is no minimum fee or setup cost.
https://docs.aws.amazon.com/kinesisanalytics/latest/dev/how-it-works.html

NO.374 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.
Answer: A

NO.375 A company is designing a new application to collect data on user behavior tor analysis at a later time Amazon Kinesis Data Streams will be used to receive user interaction events. What should be done to ensure the event data is retained indefinitely?
A. Configure the stream to write records to an attached Amazon EBS volume.
B. Configure an Amazon Kinesis Data Firehose delivery stream to store data on Amazon S3.
C. Configure the stream data retention period to retain the data indefinitely.
D. Configure an Amazon EC2 consumer to read from the data stream and store records in Amazon SQS
Answer: B

NO.376 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.
Answer: A

NO.377 A company is migrating an on-premises application to AWS. The application currently uses their corporate message broker, passing messages between layers by using the MQTT protocol. Because of time and budget constraints, the company cannot rewrite the application and cannot manage a new message broker on the EC2 instances.
Which service should a Solutions Architect use to allow the customer to migrate the application to AWS?
A. Amazon SNS
B. Amazon SQS
C. Amazon MQ
D. Amazon SWF
Answer: C
Explanation

"Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Message brokers allow different software systems-often using different programming languages, and on different platforms-to communicate and exchange information. With Amazon MQ, you can use industry standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket. You can easily move from any message broker that uses these standards to Amazon MQ because you don't have to rewrite any messaging code in your applications."

NO.378 A company needs to process a large amount of data stored in an AmazonS3 bucket. The total processing time is expected to be less than five hours. The workload cannot be interrupted and will be executed only once.
Which pricing model will ensure that job completes at the lowest cost?
A. EC2 reserved instances
B. EC2 spot block
C. EC2 On-demand Instances
D. EC2 spot fleet.
Answer: D

NO.379 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
Answer: D

NO.380 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.
Answer: B
Explanation
https://aws.amazon.com/datapipeline/

NO.381 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.
Answer: A E
Explanation
https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-ba NLB enables static IP addresses for each Availability Zone. These static addresses don't change, so they are good for our firewalls' whitelisting.

NO.382 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).

Answer: C

Explanation

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html

NO.383 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

Answer: A

Explanation

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

https://aws.amazon.com/ebs/features/

NO.384 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.

Answer: D

NO.385 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 MultiAZ.

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.

Answer: A

Explanation

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-elb-healthcheck.html

NO.386 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 tale, 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.

Answer: D

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

NO.387 A Solutions Architect has been given the following requirements for a company's VPC:
1 The solution is a two-tiered application with a web tier and a database tier.
2 All web traffic to the environment must be directed from the Internet to an Application Load Balancer.
3 The web servers and the databases should not obtain public IP addresses or be directly accessible from the public Internet.
4 Because of security requirements, databases may not share a route table or subnet with any other service.
5 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

Answer: D

Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

NO.388 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.

Answer: A

Explanation
http://infoq.com/articles/aws-vpc-cloudformation/

NO.389 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
Answer: C
Explanation
"a database that requires minimal effort to scale with a growing dataset size" rather than because index data is NoSQL (in my opinion). "Unlike RDS, DynamoDB offers push button scaling, meaning you can scale your DB on the fly, without any down time and it can be automated". If anything, SQL is more of indexing DB than DynamoDB. https://en.wikipedia.org/wiki/Database_index describes what indexed data means while
https://www.agiratech.com/the-key-differences-between-sql-and-nosql-database/ explains the difference between the two and
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.Indexes.html explains that SQL uses indexed data while DynamoDB on the other hand uses what is called "secondary index".

NO.390 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
Answer: B
Explanation
https://dzone.com/articles/confused-by-aws-storage-options-s3-ebs-amp-efs-explained

NO.391 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.
Answer: B D
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-new.html
https://aws.amazon.com/cloudwatch/faqs/
Q: Does the Amazon CloudWatch monitoring charge change depending on which type of Amazon EC2 instance I monitor?
All Amazon EC2 instance types automatically send key health and performance metrics to CloudWatch at no cost. If you enable EC2 Detailed Monitoring, you will be charged for custom metrics based on the number of metrics sent to CloudWatch for the instance. The number of metrics sent for an instance is dependent on the instance type - see available CloudWatch Metrics for Your Instances for details.

NO.392 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
Answer: C
Explanation
https://aws.amazon.com/efs/when-to-choose-efs/
https://docs.aws.amazon.com/efs/latest/ug/performance.html

NO.393 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
Answer: A
Explanation
https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/

NO.394 A solutions Architect is designing an application that stores objects encrypted in an AmazonS3 bucket. The company's security requirements state that the encryption key is stored by the organization.
Which methods meet this requirement? Select two
A. Use S3 server-side encryption with customer-provided keys
B. Use S3 client-side encryption

C. Use S3 server-side encryption with AmazonS3 managed keys
D. Use S3 server-side encryption with AWS KMS managed keys
E. Use S3 server-side encryption with the company's own keys imported into AWS KMS
Answer: A E

NO.395 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 analyze 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 analyze the data.
Answer: B
Explanation
Input - The streaming source for your application. You can select either a Kinesis data stream or a Kinesis Data Firehose data delivery stream as the streaming source. In the input configuration, you map the streaming source to an in-application input stream. The in-application stream is like a continuously updating table upon which you can perform the SELECT and INSERT SQL operations. In your application code, you can create additional in-application streams to store intermediate query result
https://aws.amazon.com/blogs/big-data/writing-sql-on-streaming-data-with-amazon-kinesis-analytics-part-1/

NO.396 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.
Answer: D
Explanation
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html

NO.397 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.
Answer: D
Explanation
https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/

NO.398 A workload is an Amazon VPC consists of an Elastic Load Balancer that distributes incoming requests across a fleet of six Amazon EC2 instances. Each EC2 instance stores and retrieves data from an Amazon DynamoDB table.
Which of the following provisions will ensure that this workload is highly available?
A. Provision DynamoDB tables across a minimum of two Availability Zones.
B. Provision the EC2 instances evenly across a minimum of two Availability Zones in two regions.
C. Provision the EC2 instances evenly across a minimum of two Availability Zones in a single region.
D. Provision the Elastic Load Balancer to distribute connections across multiple Availability Zones.
Answer: D

NO.399 An application runs in a VPC on Amazon EC2 instances behind an Application Load Balancer. Traffic to the Amazon EC2 instances must be limited to traffic from the application load balancer. Based on these Requirements, The Security group Configuration should only allow traffic from:
A. the public IPs of the Application Load Balancer nodes.
B. the ip range of the application Load Balancer Subnets.
C. the security group attached to the application load balancer.
D. the VPC CIDR.
Answer: C

NO.400 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.
Answer: C

NO.401 A startup is building an application to track the high scores for a popular video game. Their Solution Architect is tasked with designing a solution to allow real-time processing of scores from millions of players worldwide.
Which AWS service should the Architect use to provide reliable data ingestion from the video game into the datastore?
A. AWS Data Pipeline
B. Amazon Kinesis Firehose
C. Amazon DynamoDB Streams
D. Amazon Elasticsearch Service
Answer: B

NO.402 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.
Answer: C
Explanation
https://aws.amazon.com/about-aws/whats-new/2014/05/20/amazon-s3-now-supports-lifecycle-rules-for-versionin

NO.403 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.
Answer: B

NO.404 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
Answer: B

NO.405 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.
C. Configure the database subnet network ACL to deny all inbound nondatabase traffic from the application-tier subnet.
D. Configure the database subnet network ACL to allow inbound database traffic from the application-tier subnet.
Answer: B
Explanation
Configure the database security group to allow database traffic from the application server security group.
Anytime you see "Allow traffic" think Security groups

NO.406 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 file servers.
Answer: B

NO.407 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
Answer: B C

NO.408 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
Answer: B
Explanation
https://www.allthingsdistributed.com/2010/02/strong_consistency_simpledb.html
https://cloudacademy.com/blog/consistency-models-of-amazon-cloud-services/
https://aws.amazon.com/blogs/aws/amazon-rds-announcing-read-replicas/

NO.409 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)
Answer: A
Explanation
https://docs.aws.amazon.com/en_pv/efs/latest/ug/accessing-fs-nfs-permissions.html

NO.410 A customer owns a simple API for their website that receives about 1,000 requests each day and has an average response time of 50 ms. 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.
Answer: B
Explanation
Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create REST and WebSocket APIs that act as a "front door" for applications to access data, business logic, or functionality from your backend services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, any web application, or real-time communication applications. API Gateway handles all the tasks involved in accepting and

processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scale

NO.411 A Company requires scalable shared storage to be accessed from hundreds of Linux-based Amazon EC2 instances in a single region.
Which option provides the greatest levels of availability and performance?
A. Mount an Amazon S3 bucket as a volume by using third-party tools like s3fs
B. Implement a file gateway in the same region, and present it to the EC2 instances
C. Use Amazon EFS and mount it from different Availability Zones
D. Design an LVM-based NFS server, and add more Provisioned IOPS volumes to it when more space is needed
Answer: C

NO.412 A Solutions Architect needs to design an Amazon EC2 cluster to analyse data that is currently stored in Amazon S3. A key requirement is to utilize the fastest storage service available when analysing the data locally on the Amazon EC2 instance.
Which of the following storage types should the Architect choose to meet the requirement? (Answer)
A. AWS Storage Gateway
B. Amazon EBS using Provisioned IOPS(PIOPS)
C. Amazon EC2 instance (ephemeral) Store
D. Amazon Glacier
Answer: B

NO.413 A Solutions Architect is designing a new application that will be hosted on EC2 instances. This application has the following traffic requirements:
1 Accept HTTP(80)/HTTPS(443) traffic from the Internet.
2 Accept FTP(21) traffic from the finance team servers at 10.10.2.0/24.
Which of the following AWS CloudFormation snippets correctly declares inbound security group rules that meet the requirements and prevent unauthorized access to additional services on the instance?
A. [{
"IpProtocol" : "tcp",
"FromPort" : "0",
"ToPort" : "65535",
"CidrIp" : "10.10.2.0/24"
}, {
"IpProtocol" : "tcp",
"FromPort" : "443",
"ToPort" : "443",
"CidrIp" : "0.0.0.0/0"
},
{
"IpProtocol" : "tcp",

"FromPort" : "80",
"ToPort" : "80",
"Cidrlp" : "0.0.0.0/0"
}]

B. [{
"IpProtocol" : "tcp",
"FromPort" : "21",
"ToPort" : "21",
"Cidrlp" : "10.10.2.0/18"
}, {
"IpProtocol" : "tcp",
"FromPort" : "443",
"ToPort" : "443",
"Cidrlp" : "0.0.0.0/0"
},
{
"IpProtocol" : "tcp",
"FromPort" : "80",
"ToPort" : "80",
"Cidrlp" : "0.0.0.0/0"}]

C. [{
"IpProtocol" : "tcp",
"FromPort" : "443",
"ToPort" : "443",
"Cidrlp" : "0.0.0.0/0"
},
{
"IpProtocol" : "tcp",
"FromPort" : "80",
"ToPort" : "80",
"Cidrlp" : "0.0.0.0/0"
},
{
"IpProtocol" : "tcp",
"FromPort" : "21",
"ToPort" : "21",
"Cidrlp" : "10.10.2.0/24"
}]

D. [{
"IpProtocol" : "udp",
"FromPort" : "443",
"ToPort" : "443",
"Cidrlp" : "0.0.0.0/0"
},
{
"IpProtocol" : "udp",

"FromPort" : "80",
"ToPort" : "80",
"Cidrlp" : "0.0.0.0/0"
},
{
"IpProtocol" : "udp",
"FromPort" : "21",
"ToPort" : "21",
"Cidrlp" : "10.10.2.0/24"
}]

Answer: C

Explanation

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-security-group-ingress

NO.414 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 first 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 STANDARDJA 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 STANDARDJA 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.

Answer: D

Explanation

https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

NO.415 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 first.

C. Trigger a Lambda function when a new object is uploaded.

D. Initially copy the images to an attached Amazon EBS volume.

Answer: A

NO.416 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.
Answer: A
Explanation
https://medium.com/tensult/disaster-recovery-2dd15bea9d39

NO.417 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
Answer: B D
Explanation
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Performance.html

NO.418 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.
Answer: C
Explanation
"Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments"

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

NO.419 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.

Answer: A

Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service.html
"You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an endpoint service). Other AWS principals can create a connection from their VPC to your endpoint service using an interface VPC endpoint. You are the service provider, and the AWS principals that create connections to your service are service consumers."

NO.420 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.

Answer: D

Explanation
https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html

NO.421 A Solutions Architect is designing a new web application on Amazon EC2. The system must make application-specific metrics, such as application security events, available to the SysOps teams. How should the solutions Architect enable this in the design?

A. Install AWS SDK on the application instances. Design the application to use the AWS SDK to log events directly to an Amazon S3 bucket

B. Install the Amazon Inspector agent on the application instances. Design the application to store

events m application log files

C. Install the Amazon CloudWatch Logs agent on the application instances. Design the application to store events in application log files

D. Install AWS SDK on the application instances. Design the application to use AWS SDK to log sensitive events directly to AWS CloudTrail

Answer: C

Explanation

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html

NO.422 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.

Answer: C

NO.423 A development team is building an application with front-end 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.

Answer: C

NO.424 A Solutions Architect is designing a shared files 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. Redis Auth

B. AWS Single Sign-On

C. IAM database authentication

D. VPC security group for Redis

Answer: A

NO.425 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
Answer: C

NO.426 An application must access data in an Amazon RDS Aurora DB instance.
Which methods will allow this? (Select TWO)
A. Retrieve credentials from AWS KMS.
B. Create a user in the database.
C. Enable IAM database authentication
D. Enable AWS Security Token Service
E. Create a user in the database parameter group
Answer: B C

NO.427 An on-premises application publishes messages to an Amazon SQS queue.
What is the MOST secure way to provide security credentials to the application?
A. Store the credentials in AWS Systems Manager Parameter Store
B. Include an IAM user's access key and secret access key in the application code.
C. Keep an IAM user's access key and secret access key encrypted in a file
D. Launch the instance with an IAM role
Answer: B

NO.428 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
Answer: B

NO.429 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.

Answer: C

NO.430 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

Answer: B

Explanation

https://aws.amazon.com/rds/aurora/customers/

NO.431 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.

Answer: A

Explanation

https://aws.amazon.com/premiumsupport/knowledge-center/create-read-replica-rds/

NO.432 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 onpremises 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 onpremises datacenter.
D. Use HTTPS for traffic over gateway VPC endpoints that have been configured for the Amazon EC2 instance.
Answer: C

NO.433 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
Answer: C

NO.434 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
Answer: C

NO.435 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
Answer: A B
Explanation

https://www.reddit.com/r/aws/comments/ap2haa/cloudfront_cheaper_than_alb/
"It probably ends up cheaper because you can take advantage of the CDN element, caching assets like images, css, js etc on CloudFront rather than having all traffic traverse the ALB to retrieve them. If you already use a CDN for these then you may not see any cost benefit adding it into the mix.
We also use CloudFront for SSL termination of 30+ customer sites, with a single ALB serving requests to the back end. We were using a separate CDN provider but we're moving all our assets into CloudFront too because it's going to end up way cheaper."

NO.436 A solutions architect is architecting a workload that requires a highly available shared block file storage system that must be consumed by multiple Linux applications. Which service meets this requirement?
A. Amazon EFS
B. AmazonS3
C. AWS storage gateway
D. Amazon EBS
Answer: A

NO.437 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.
Answer: B
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/deleteontermination-ebs/

NO.438 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
Answer: A

NO.439 An online retailer has a series of flash sales occurring every Friday Sales traffic will increase during the sales only and the platform will handle the increased load. The platform is a three-tier application The web tier runs on Amazon EC2 instances behind an Application Load Balancer. Amazon CloudFront is used to reduce web server load, but many requests for dynamic content must go to the web servers.
What should be done to the web tier to reduce costs without impacting performance or reliability?
A. Use T-series instances.

B. Purchase scheduled Reserved Instances.
C. Implement Amazon ElastiCache.
D. Use Spot Instances.
Answer: B

NO.440 A Solutions Architect is designing the architecture for a web application that will be hosted on AWS. Internet users will access the application using HTTP and HTTPS.
How should the Architect design the traffic control requirements?
A. Use a network ACL to allow outbound ports for HTTP and HTTPS Deny other traffic for inbound and outbound
B. Use a network ACL to allow inbound ports for HITP and HTTPS Deny other traffic for inbound and outbound
C. Allow inbound ports for HTTP and HI IPS in the security group used by the web servers
D. Allow outbound ports for HTTP and HTTPS in the security group used by the web servers
Answer: C
Explanation
https://d1.awsstatic.com/whitepapers/aws-web-hosting-best-practices.pdf

NO.441 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.
Answer: A
Explanation
Step Scaling Policies for Application Auto Scaling With step scaling, you choose scaling metrics and threshold values for the CloudWatch alarms that trigger the scaling process as well as define how your scalable target should be scaled when a threshold is in breach for a specified number of evaluation periods.
Step scaling policies increase or decrease the current capacity of a scalable target based on a set of scaling adjustments, known as step adjustments. The adjustments vary based on the size of the alarm breach.

NO.442 A media company has more than 100TB 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
D. Amazon S3 Standard Infrequent Access

Answer: D

NO.443 A Solutions Architect is architecting a workload that requires a performant objectbased 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
Answer: B
Explanation
https://aws.amazon.com/s3/

NO.444 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.
Answer: C D
Explanation
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/authentication-and-access-control.html

NO.445 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.
Answer: C E
Explanation
https://docs.aws.amazon.com/autoscaling/ec2/userguide/healthcheck.html

NO.446 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

Answer: C

Explanation

"Your on premises server has application using proprietary file system. How do you migrate to AWS? The Answer: Use EBS volumes with EC2. Other choices included EFS, Stored Volumes etc. Keyword is proprietary file system since EFS supports NFS and stored volumes support iSCSI".

http://knowledgehills.com/aws/my-day-at-aws-csaa-exam.htm

NO.447 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 a Amazon DynamoDB table.

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.

Answer: A

Explanation

https://docs.aws.amazon.com/apigateway/latest/developerguide/setup-http-integrations.html

NO.448 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

Answer: D