QUESTION 1
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
Amazon Redshift protects data at rest through encryption. To manage the keys used for encrypting and decrypting your Amazon Redshift resources, you use AWS Key Management Service (AWS KMS). AWS KMS combines secure, highly available hardware and software to provide a key management system scaled for the cloud.

QUESTION 2
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
Amazon SQS - whenever its decoupled, answer is SQS

QUESTION 3
A legacy application needs to interact with local storage using iSCSI. A team needs to design a reliable storage solution to provision all new storage on AWS.

Which storage solution meets the legacy application requirements?

A. AWS Snowball storage for the legacy application until the application can be re-architected.
B. AWS Storage Gateway in cached mode for the legacy application storage to write data to Amazon S3.
C. AWS Storage Gateway in stored mode for the legacy application storage to write data to Amazon S3.
D. An Amazon S3 volume mounted on the legacy application server locally using the File Gateway service.

Answer: C

Question here is -- where you want to store the data? in AWS ...
Explanation :

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

More detail

What is Volume Gateway?

A: Volume Gateway provides an iSCSI target, which enables you to create block storage volumes and mount them as iSCSI devices from your on-premises or EC2 application servers. The Volume Gateway runs in either a cached or stored mode.

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access.
In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

In either mode, you can take point-in-time snapshots of your volumes, which are stored as Amazon EBS Snapshots in AWS, enabling you to make space-efficient versioned copies of your volumes for data protection, recovery, migration and various other copy data needs.

it needs to provision all new storage on AWS. Cached mode doesn't store entire data but only frequently accessed data.

QUESTION 4
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
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

QUESTION 5
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

Redshift is a data warehouse. As the question states that the application cannot allow downtime for schema change, NoSQL DB is the only option and which is Dynamo DB.

QUESTION 6
A Solutions 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

the question refers to Disaster Recovery, and not high availability.
Redshift uses CROSS-REGIONAL SNAPSHOTS. Also 500 miles is obviously regional because Availability zones are always around 60miles

QUESTION 7
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

Why? Here there are asking to download the whole object(Not in parts) so the correct answer is D only..
Why "A" is wrong"(here retrieval in parts)
For GETs, range http header can help to improve the downloads by allowing the object to be retrieved in parts instead of the whole object quick recovery from failures, as only the part that failed to download needs to be retried

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

QUESTION 8
A Solutions Architect is designing a new social media application. The application must provide a secure method for uploading profile photos. Each user should be able to upload a profile photo into a shared storage location for one week after their profile is created.
Which approach will meet all of these requirements?

A. Use Amazon Kinesis with AWS CloudTrail for auditing the specific times when profile photos are uploaded.
B. Use Amazon EBS volumes with IAM policies restricting user access to specific time periods.

C. Use Amazon S3 with the default private access policy and generate pre-signed URLs each time a new site profile is created.

D. Use Amazon CloudFront with AWS CloudTrail for auditing the specific times when profile photos are uploaded.

Answer: C

Use pre-signed URL (basically an API) that you can define and set an expiration on and many other parameters for users or entities that don't have AWS credentials to access objects in Amazon S3
Pre-Signed Url is the key here
The presigned URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions.
https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html

QUESTION 9
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

EBS is block storage. EFS is not block storage and EFS makes use of burst, so its not continuously on 100 MiB/s. https://docs.aws.amazon.com/efs/latest/ug/performance.html

Checked the web site from AWS. EFS is a file storage service.
From AWS:
Amazon EFS provides scalable file storage for use with Amazon EC2. You can create an EFS file system and configure your instances to mount the file system.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEFS.html

EBS is the only block storage available in AWS. so the read/write operations doesn't matter. it clearly says block storage, So the Answer is **C**

A. Amazon S3 ----------- Object Storage
B. Amazon EFS ------------- File System
C. Amazon EBS ---------- ***Block Storage
D. Amazon Glacier ---------- Long term Storage solution, Achieve.

QUESTION 10
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
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.

question state,
30 days rarely use ------- Amazon S3 Standard Infrequent Access
After 60 days no use again -------------- Glacier storage

QUESTION 11
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,
DynamoDB Note, Key pair, Unstructured, Semi-Structure.
Keywords such as "key-value pair" and "semi-structured documents" are obvious and leading us too DynamoDB.

QUESTION 12
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? (Choose two.)

A. **Create a VPC Endpoint for Amazon RDS.**
B. **Create the Lambda function within the Amazon RDS VPC.**
C. **Change the ingress rules of Lambda security group, allowing the Amazon RDS security group.**
D. **Change the ingress rules of the Amazon RDS security group, allowing the Lambda security group.**
E. **Add an Internet Gateway (IGW) to the VPC, route the private subnet to the IGW.**

Answer: BD
Definitely B & D. There are VPC endpoints, but they don't support Lambda. There is a tutorial on Amazon's website that shows you how to set this up. It requires a Lambda function to be created along with the VPC subnet parameters where the RDS instance is located. https://docs.aws.amazon.com/lambda/latest/dg/services-rds-tutorial.html

All you need is create a vpc endpoint (interface) for Lambda in the VPC where RDS instance is in. Then Lambda is the source and RDS is the destination. Hence pick the related option for security groups.
it's B & D: https://aws.amazon.com/blogs/aws/new-access-resources-in-a-vpc-from-your-lambda-functions/

QUESTION 13
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
As part of our plan to make it even easier for you to build and run AWS applications that have a global footprint, I am happy to announce that Amazon Redshift now has the ability to automatically back up your cluster to a second AWS region!

You simply select the second region and the desired retention period; Redshift will take care of the rest:
Once you enable this feature, Redshift will make subsequent snapshots available in the second region.
— Jeff;
https://aws.amazon.com/blogs/aws/automated-cross-region-snapshot-copy-for-amazon-redshift/

https://aws.amazon.com/blogs/aws/automated-cross-region-snapshot-copy-for-amazon-redshift/

QUESTION 14
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

Reason: One of the ways to improve the performance of your Aurora primary DB is to create read replicas and use a reader endpoint to load balance between the replicas.
A is wrong : Redshift is a Datawarehouse not a conventional relational DB
B is wrong: Cloudfront has got nothing to do with Aurora RDS
C: They already clearly said its running on the largest instance size, meaning its already using EBS Provisioned iops

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability...
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html#Aurora.Replication.Replicas

QUESTION 15
Solutions Architect is designing the architecture for a new three-tier web-based e-commerce site that must be available 24/7. Requests are expected to range from 100 to 10,000 each minute. Usage can vary depending on time of day, holidays, and promotions. The design should be able to handle these volumes, with the ability to handle higher volumes if necessary.
How should the Architect design the architecture to ensure the web tier is cost-optimized and can handle the expected traffic? (Choose 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.
To handle traffic = Autoscaling + ELB
To cost optimize = Cloudfront
They want Cost Optimization and Handle Traffic...
Cloudfront is the best option for cost here, and Autoscaling behind ELB to handle and improve traffic

QUESTION 16
A Solutions 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 non-database traffic from the application-tier subnet.

D. Configure the database subnet network ACL to allow inbound database traffic from the application-tier subnet.

Answer: B

- Because you can spam a security group across zones and attach it to the auto scaling group so you do not need to take care of subnets of instances. And you only need to allow traffic. In a NACL you need and inbound and outbound rule.
- Security groups are stateful and required for db,application instance access configuration.
- NACL's are stateless not suitable for database,application..etc
- The best option here is B because you do not know IP of new instances in Auto Scaling group

QUESTION 17
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
NAT instance poses single point of failure
NAT instance is a Single EC2 instance. This instance has no redundancy, so NAT instance would be the single point of failure.

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.

single point of failure

B is the most correct answer. Here is AWS again writing ridiculous questions. The question does not clearly say the ELB Classic Load Balancer is deployed in multi-AZ so we can assume it is based on the question saying "An ELB Classic Load Balancer is deployed in front of the web tier and the web application tier are deployed evenly across two Availability Zones". We can deduce that only one NAT instance is launched for Amazon EC2 instances and database resources. The link below explains it very well:

https://www.botmetric.com/blog/eliminating-single-points-of-failures-on-aws-cloud/
"The best way to handle this situation is to start with identifying whether your ELB is single AZ or multiple AZ, as single AZ ELB is also considered as one of the Single Points of Failures on AWS Cloud". "Single NAT Instance in Network is a single point of failure".

QUESTION 18
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 Solutions 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
You need to mitigate the risk ok the overload at 9am. So best be sure to set up the schedule to spin up before everyone starts working.

QUESTION 19
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 of future product launches.

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: C

A and B both work with cloudwatch metrics
Scheduled scaling Action
Scheduled scaling allows you to set your own scaling schedule. For example, let's say that 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 actions based on the predictable traffic patterns of your web application. Scaling actions are performed automatically as a function of time and date.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

When questions give you the time of the spike and mention anticipation, you want to go with answers that mention scheduling. It's too late when the spike hits and your ASG is over here trying to install AMIs on EC2 instances, maybe even waiting for some cooldown period. Your manager is gonna be angry, especially when they said they wanted it a week in advance...

QUESTION 20
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

The question has 2 hints. API (so use API gateway) and the average response time is 50s (so use Lambda because it has a max response of 15 minutes).

What's your reasoning around this?

I also thought B because of the following:
Lambdas cost is transaction based. super cheap and has High availability

1st 1 million requests are free
https://aws.amazon.com/lambda/pricing/

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

QUESTION 21
A Solutions 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

To make it even easier for you to build AWS applications that span regions, we’re introducing a new EBS Snapshot Copy feature today. You can now copy EBS snapshots between EC2 Regions.

Why Copy?

So, why would you want to copy an EBS Snapshot from one AWS Region to another? Here are some of the more common use cases:

Geographic Expansion – You want to be able to launch your application in a new Region.
Migration – You want to be able to migrate your application from one Region to another.
Disaster Recovery – You want to back up your data and your log files across different geographical locations at regular intervals to minimize data loss and recovery time.
EBS Snapshot Copy simplifies each of these use cases by simplifying the copy process.

QUESTION 22
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

QUESTION 23
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
Cloudwatch has a few default metrics it uses to monitor your VPN end to end connection. One of them is the Tunnelstate Metric

You can monitor VPN tunnels using CloudWatch, which collects and processes raw data from the VPN service into readable, near real-time metrics. These statistics are recorded for a period of 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. VPN metric data is automatically sent to CloudWatch as it becomes available.

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

QUESTION 24
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
There are 2 default ways to improve the performance of your RDS primary instance. 1 is in-memory cache (Redis or memcached) Elasticache and 2 is read replicas using asynchronous replication from your primary and you can offload read queries to them. PostGreSQL, MariaDB and MySQL is supported.
Since RDS is autoscale already, use Elasticache to improve the performance

QUESTION 25
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
A VPC endpoint enables you to create a private connection between your VPC and another AWS service without requiring access over the Internet

New VPC Endpoint for S3
Today we are simplifying access to S3 resources from within a VPC by introducing the concept of a **VPC Endpoint. These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances.
https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/

QUESTION 26
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

Once you see OLTP (transaction processing DB), I/O intensive DB the most consistent EBS storage is provisioned IOPS

QUESTION 27
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)**

Answers: C
keyword "log-processing, sequentially"

QUESTION 28
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

Add a date as the prefix.

You no longer have to randomize prefix naming for performance, and can use sequential date-based naming for your prefixes

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

You will read the line "You no longer have to randomize prefix naming for performance, and can use sequential date-based naming for your prefixes." . it is a best practice.

QUESTION 29

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

Once you enable Cloudtrail on a root account, it will log all API interactions on the account and it will also propagate automatically to any new region defined in the account

Cloudtrail is all about insights on "API Calls" against your VPC. Please read => https://aws.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-regions-and-support-for-multiple-trails/

QUESTION 30

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

Proprietary file system mean that is owned and copyrighted, and that there are limitations against use, distribution and modification

2)Like NTFS or fat32 in Windows systems. Those are owned by Microsoft.

3)EFS is it's own thing, and AWS manages the "file system" being used and can't be mapped in windows ec2 instance

QUESTION 31

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

ECS for container, Reserved Instance for Critical Load, and Spot for Non Critical Load

What is an ECS?

Amazon Elastic Container Service (ECS) is a cloud computing service in Amazon Web Services (AWS) that manages containers and allows developers to run applications in the cloud without having to configure an environment for the code to run in. ... ECS supports Docker, an open source Linux container service.

One Critical for Reserved

One NOn Critical for Spot

ECS is a great choice to run containers for several reasons.

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

QUESTION 32

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

QUESTION 33

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: A

the question was "which storage should a Solutions...." Answer is A. S3 is a storage solution. RDS is not a storage solution, it's service that uses block storage and S3 storage.

QUESTION 34
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

Not Lambda@Edge
https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html

We need "AWS-managed service": Lambda@Edge is a feature, not "AWS-managed service". You have to create AWS Lambda first, then Lambda@Edge

QUESTION 35
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
AWS SQS FIFO Queue
SQS FIFO Queue provides enhanced messaging between applications with the additional features
FIFO (First-In-First-Out) delivery
order in which messages are sent and received is strictly preserved
key when the order of operations & events is critical
Exactly-once processing
a message is delivered once and remains available until a consumer processes and deletes it
key when duplicates can’t be tolerated. limited to 300 transactions per second (TPS)

QUESTION 36
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

B. Encrypt Amazon EBS volumes on Amazon EC2 instances - **Block Storage**

C. Enable server-side encryption on Amazon S3 - **Object Storage**

D. Encrypt Amazon EC2 Instance Storage – **Computing**

QUESTION 37
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
(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.

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingHostedZone.html

info: Amazon Route 53 is a great way to manage all of your DNS services from a modern cloud infrastructure. You can use it to register new domains, manage existing ones, route traffic both to AWS hosted DNS servers and 3rd party servers, as well as handle failover to backup services

Can I point my zone apex (example.com versus www.example.com) at my Amazon CloudFront distribution? 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 your Amazon CloudFront distribution (for example, d123.cloudfront.net).

QUESTION 38
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 HDD volumes.

Answer: A

A Amazon Kinesis Data Firehose

real-time streaming (Every 5 minute) which is the simplest

No need to think, the Answer is A, Kinesis is the only database that can support streaming data.

QUESTION 39
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
Bank transactions -> OLTP -> SQL database -> Aurora/RDS
Redshift is SQL too but it is a data warehouse not database used for OLTA primarily
Amazon Aurora is RDB where you can join tables together and do other administrative cool stuff , meanwhile S3 is storage for Object ,Redshift is for Data Wearhouse and DynamoDB is NoSQL Database

QUESTION 40
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
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.

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

QUESTION 41
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.

Asnwer: A
What did it for me is this statement "uploading images through the web server will create too much traffic". Simply don't go through the web server, go directly. Sign the url so it is only open to those from the web server.

The presigned URLs can be generated programmatically and upload also happens programmatically. Presigned URL is a keyword to look for when uploading objecta through a web app by users without aws credentials..

knowledge : difference between cloudwatch and cloudtrail
CloudWatch is a monitoring service for AWS resources and applications. CloudTrail is a web service that records API activity in your AWS account. ... CloudTrail is also enabled by default when you create your AWS account. With CloudWatch, you can collect and track metrics, collect and monitor log files, and set alarms

QUESTION 42

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.

Asnwer: A

Because flow logs is the only service the allows you to mointor the follow of the Network IP Addresses.
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
keywords 'records logs', 'private vpc'

Diff b/w Cloudwatch and Cloud Trail??

QUESTION 43
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.

Asnwer: BE

Auto scaling is done with ASG for the weak back end, and the reverse proxy bottleneck is solved by replacing both the front end Classic ELB and the backend proxy with a single Application ELB

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

QUESTION 44
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

T he website will go up tomorrow. No one is going to migrate a DB to a brand new, untested platform over night before opening day. The answer is C. Autoscaling is the easiest thing to do the nigh before opening day and you can do this for the all tiers of the app if needed.

QUESTION 45

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

Use CouldFront to Distribute the traffic accordingly

keyword is static content-> cloud front distribution is best option

QUESTION 46

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

How to migrate NAT instances to NAT gateway?

For NAT instances: Use a script

For NAT gateway, Launch a NAT gateway in each Availability Zone.

QUESTION 47

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

Amazon S3 Transfer Acceleration

https://aws.amazon.com/blogs/aws/aws-storage-update-amazon-s3-transfer-acceleration-larger-snowballs-in-more-regions/

QUESTION 48
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

Kinesis FireHose is used to analyze the streaming data. But in question, there is nothing mentioned regarding Analysis. So the best answer is D. API Gateway is the entry point to AWS.

QUESTION 49
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

you must always create your NAT gateway in a public subnet that already has a defined route to 0.0.0.0/0 through an internet gateway. and assign an Elastic IP to the NAT gateway

Keyword = NAT for Private to Public communication, NAT Gateway & Instance always on Public Subnet

QUESTION 50
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

The application servers and database must be secure. so it must me in private subnet. In question itself we have answer. ELB already in public subnet .Elb will communicate to private subnet.

the only thing is that All subnets must be in the same AZ.

ELB > Public Subnet > AZ1

EC2s > Private Subnet > AZ1

RDS > Private Subnet > AZ1

https://www.google.com/amp/s/blog.stratus10.com/aws-best-practices-3-tier-infrastructure%3fhs_amp=true

QUESTION 51

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 is D.
It requires throughput up to 500 MB/s and cold HDD can provide only upto 250 MB/s.
https://aws.amazon.com/blogs/aws/amazon-ebs-update-new-cold-storage-and-throughput-options/ Throughput Optimized HDD (st1) – Designed for high-throughput MapReduce, Kafka, ETL, log processing, and data warehouse workloads; $0.045 / gigabyte / month. Cold HDD (sc1) – Designed for workloads similar to those for Throughput Optimized HDD that are accessed less frequently; $0.025 / gigabyte / month.

Keywords sequentially accessed, streaming data = throughput optimized

QUESTION 52

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: C

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-content-encodings-examples-image-s3.html
https://aws.amazon.com/api-gateway/faqs/

https://www.humansreadcode.com/api-gateway-ip-whitelisting/

QUESTION 53

A Solutions Architect is designing a database solution that must support a high rate of random disk reads and writes. It must provide consistent performance, and requires long-term persistence. Which storage solution BEST meets these requirements?

A. An Amazon EBS Provisioned IOPS volume
B. An Amazon EBS General Purpose volume
C. An Amazon EBS Magnetic volume
D. An Amazon EC2 Instance Store

Answer: A

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html General Purpose SSD (gp2) Use Cases: Recommended for most workloads, System boot volumes, Virtual desktops, Low-latency interactive apps, Development and test environments.

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

Provisioned IOPS. Keywords: consistent performance, database, High I/O

QUESTION 54
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

QUESTION 55
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

QUESTION 56
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
Because Egress-only Internet Gateway be able to access the Internet, but prevent resources on the Internet from initiating communication with your instance. https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html
Using a NAT Gateway because the DB servers (located in private subnet) wants to connect to Internet for software updates then it must go through a NAT Gateway (configured to forward traffic to the Internet)

QUESTION 57
A Solutions Architect is designing a Lambda function that calls an API to list all running Amazon RDS instances.
How should the request be authorized?

A. Create an IAM access and secret key, and store it in the Lambda function.
B. Create an IAM role to the Lambda function with permissions to list all Amazon RDS instances.
C. Create an IAM role to Amazon RDS with permissions to list all Amazon RDS instances.
D. Create an IAM access and secret key, and store it in an encrypted RDS database.

Answer:B

WS service to service interaction withouht the need to create credentials, we use AWS IAM Roles. in this case we define a policy list RDS instances, use it to create a role and attach the role to the Lambda function https://docs.aws.amazon.com/lambda/latest/dg/vpc-rds.html

QUESTION 58

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

Because only Provisioned IOPS type EBS support more than 16000 IO per volume. Requirement is 20000.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/requesting-ebs-volume-modifications.html

QUESTION 59

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

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

I walk through an approach for building such an index using Amazon DynamoDB and AWS Lambda. With these technologies, you can create a high performance, low-cost index that scales and remains highly available without the need to maintain traditional servers."

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

QUESTION 60

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

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

B. Move the website to Amazon S3. -- move to S3 does not provide the HA C. Change the ELB to an Application Load Balancer. ----ALB and Classic LB no different, they are the samething. only different is ALB can do advanced route like:Path, host. D. Move some Amazon EC2 instances to a subnet in the same Availability Zone. ---- in the same Availability Zone? how to get HA? so not right.

QUESTION 61

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? (Choose 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: CD

Create IAM role + assign role to EC2. -->> https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/authentication-and-access-control.html

QUESTION 62

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? (Choose 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: BC

B to collect per day sensitive data details D because per the second metric only allowed for "Currently, only custom metrics that you publish to CloudWatch are available at high resolution with Detailed Monitoring enabled for EC2." So anyway enable Detailed Monitoring is the first step. (Looks partial but closet one) To be honest, options are not completely appropriate. It should be "Create custom metrics" and "Enable detailed monitoring." A and E are rubbish. C says about custom ALARMS but not custom METRICS.

QUESTION 63

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

QUESTION 64

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

Becuase RDS MySQL is in Private Subnet and with security group linked to webserver instance in Public Subnet

SG is at the instance level and NACL is at the subnet level. Editing any NACL can impact other applications at the subnet level. I used process of elimination anything NACL then looked closer to the SG answers.

QUESTION 65
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

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

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

QUESTION 66
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

Good explanation here; https://www.edureka.co/community/2813/aws-autoscaling-without-elastic-load-balancing

Users access only ELB to access the application and it ELB who decide where to send traffic on the registered EC2 instances based on workload.

QUESTION 67
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

https://aws.amazon.com/microservices/ Elastic Load Balancing Application Load Balancer The Application Load Balancer load balances HTTP and HTTPS traffic at the application layer (level 7) providing advanced request routing that is targeted at the delivery of modern application architectures, including microservices and containers.

Elastic Load Balancer https://docs.aws.amazon.com/aws-technical-content/latest/microservices-on-aws/microservices-on-aws.pdf?icmpid=link_from_whitepapers_page

QUESTION 68

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

What is striped volume raid0?

Summary. A striped volume (RAID 0) combines areas of free space from multiple hard disks (anywhere from 2 to 32) into 1 logical volume. Data that is written to a striped volume is interleaved to all disks at the same time instead of sequentially.

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/

A. Store data in a filesystem backed by Amazon Elastic File System (EFS). Incorrect. Would have been ideal if application runs on several EC2

B. Store data in Amazon S3 and use a third-party solution to expose Amazon S3 as a filesystem to the database server. Incorrect. S3 is an object storage.

C. Store data in Amazon Dynamo DB and emulate relational database semantics. Incorrect. "...The database will run on Amazon EC2."

D. Stripe data across multiple Amazon EBS volumes using RAID 0. Correct!

Keyword "Hosted on EC2 and we know EC2 uses block storage =EBS. Plus RAID 0 increases performance

QUESTION 69

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

An egress-only Internet gateway is stateful: it forwards traffic from the instances in the subnet to the Internet or other AWS services, and then sends the response back to the instances.

A. an egress-only internet gateway
most simplest question...... egress is for IPV6
while Nat Gateway is for IPV4

QUESTION 70
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
Aurora uses read replica to improve performance of the primary DB instance and offload read queries to the read replicas. the reader endpoint balances load to the replicas

QUESTION 71
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

QUESTION 72
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

QUESTION 73
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

Keywords: stateful web application = needs constant storage to hold different types of data including session data. Highly Availible and cheapest = Standard reserved

standard reserved, it is worth mentioning that scheduled reserved would probably be much cheaper than standard if the time scheduled was low. So even if you are paying more per hour, if the hours are few, you would potentially pay much less than paying for 24 hours every day. So the key here is the consistent workload.

QUESTION 74
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

Amazon EFS

Keyword here is POSIX-compliant and EFS support multiple EC2 Instances.

QUESTION 75
A Solutions 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: AC

QUESTION 76
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

Use encrypted EBS storage volumes with AWS-managed keys.

since the app is deploy using EBS and no changes require

Amazon EBS encryption offers a straight-forward encryption solution for your EBS resources that doesn't require you to build, maintain, and secure your own key management infrastructure. It uses AWS Key Management Service (AWS KMS) customer master keys (CMK) when creating encrypted volumes and snapshots.

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

QUESTION 77

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

QUESTION 78

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

Since disk performance is blocking, increasing disk performance with provisioned IOPS should be the solution. Bursting EC2 is bursting compute power

Burstable performance instances can burst CPU to a higher level. But the question asks for a solution to improve database performance using persistent storage

Keyword : Legacy, Persistent Storage, Performance..So IOPS. Question never mentioned anything other than performance or storage related to CPU or Burstable related

QUESTION 79

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

Amazon Kinesis Stream. https://aws.amazon.com/blogs/big-data/create-real-time-clickstream-sessions-and-run-analytics-with-amazon-kinesis-data-analytics-aws-glue-and-amazon-athena/

You can use Kinesis in any situation that calls for large-scale, real-time data ingestion and processing. Logs for servers and other IT infrastructure, social media or market data feeds, web clickstream data, and the like are all great candidates for processing with Kinesis.
Not SQS FIFO queue cos they can only process 300 transactions per second,

QUESTION 80
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
RDS max db size is 16TB for Aurora max is 64TB the inital db is 6 TB of data and will grow exponentially.

Please see this logic. On Premise transactional database is always relational data based so it should not be migrated to DynamoDB which is non-relational Database. The only choice left is RDS which Aurora or MySQL. Aurora is time faster than MySql and starts from 6TB. Hence correct answer is Aurora.

QUESTION 81
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: AC

Good find! This explains why the answer would be answer is A + C rather than A + E.

A = Inbound on Port 443 is fine as Security Groups are stateful (allow the traffic to return to the remote party without an explicit rule)
C = Inbound 443 on the Network ACL is a given, however, Network ACL's are stateless and therefore need configuring. In this case, the web server replies on a range of ports and therefore it is required that they are all open rather than simply 443 as stated in answer E.

You MUST enable ephemeral ports in range 32768-65535 for HTTP/S or TCP traffic will not make it back. Since this has not been offered, custom TCP outbound rule 0.0.0.0/0 will do the job. You can read details here: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports

QUESTION 82
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
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

QUESTION 83
A Solutions Architect is architecting a workload that requires a performant object-based storage system that must be shared with multiple Amazon EC2 instances.

Which AWS service meets this requirement?

A. Amazon EFS
B. Amazon S3
C. Amazon EBS
D. Amazon ElastiCache

Answer : B

Object Based = S3

Keyword "Shared" and not "attached"
QUESTION 84
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

QUESTION 85
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
"small I/O" = SSD

QUESTION 86
As part of securing an API layer built on Amazon API gateway, a Solutions Architect has to authorize users who are currently authenticated by an existing identity provider. The users must be denied access for a period of one hour after three unsuccessful attempts.

How can the Solutions Architect meet these requirements?

A. Use AWS IAM authorization and add least-privileged permissions to each respective IAM role.

B. Use an API Gateway custom authorizer to invoke an AWS Lambda function to validate each user's identity.

C. Use Amazon Cognito user pools to provide built-in user management.

D. Use Amazon Cognito user pools to integrate with external identity providers.

Answer: B

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.

Reason? you can customize API/LAMDA to meet your requirements https://aws.amazon.com/blogs/compute/introducing-custom-authorizers-in-amazon-api-gateway/

https://www.alexdebrie.com/posts/lambda-custom-authorizers/ * multiple link available via google search

QUESTION 87

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

Pictures and videos are static data and CloudFront is the most effective solution for caching static data.
because the content is on-premise. "ElastiCache currently allows access only from the EC2 network and cannot be accessed from outside networks like on-premises servers" (http://jayendrapatil.com/aws-elasticache-certification/).
CloudFront on the other hand can be used for on-premise content because "Another important aspect that not many people realise, is that the source data need not be on AWS. Yes, that's correct, your source files could be on an on-premise server, in another local datacentre, or even on Azure." (https://kaskade.cloud/amazon-cloudfront-is-here-now-what/).
Also, "When using an on-premise or non-AWS based web server you must specify the DNS name, ports and protocols that you want CloudFront to use when fetching objects from your origin." (https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/).

QUESTION 88

A client notices that their engineers often make mistakes when creating Amazon SQS queues for their backend system.

Which action should a Solutions Architect recommend to improve this process?

A. Use the AWS CLI to create queues using AWS IAM Access Keys.

B. Write a script to create the Amazon SQS queue using AWS Lambda.

C. Use AWS Elastic Beanstalk to automatically create the Amazon SQS queues.

D. Use AWS CloudFormation Templates to manage the Amazon SQS queue creation.

Answer:D

QUESTION 89
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

QUESTION 90
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: C
HDD is cheaper than SDD and HDD has a high throughput which is needed for sequential reads. Check out https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html which shows that st1 (HDD) has higher throughput than gp2 (SSD).

keyword hint: a big data application, very high sequential I/O, Low-cost therefore it is C refer use case :

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

QUESTION 91
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

QUESTION 92
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: AC
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.

What is AWS SNS used for?
Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. In Amazon SNS, there are two types of clients—publishers and subscribers—also referred to as producers and consumers.

QUESTION 93
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

QUESTION 94
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: C

QUESTION 95
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 interface 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

QUESTION 96
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
QUESTION 97
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 : B
the key in this question is: "ensure that when an application uploads an object to the Amazon S3 bucket, the object is encrypted" so you need to make sure that the object is encrypted when uploading an object in order to approve the upload, this can be done using bucket policy.

C is incorrect as the question is asked to make sure the object is encrypted while upload. If the default encryption is enabl ed, you still can upload unencrypted obj to the bucket. Although the object will be encrypted after uploading, it doesn't ensure any object is encrypted before upload. The question is to ensure that the object is encrypted when application upload the object. So C is incorrect. B is correct, you can set a bucket policy to deny PutObject API call to S3 without encryption. The link below has policy example: https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/
https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/
Amazon S3 evaluates and applies bucket policies before applying bucket encryption settings. Even if you enable bucket encryption settings, your PUT requests without encryption information will be rejected if you have a bucket policies to reject such PUT requests. Check your bucket policy and modify it if required. See "Default Encryption" warning while enabling it from the S3 Properties. https://docs.aws.amazon.com/AmazonS3/latest/user-guide/default-bucket-encryption.html

QUESTION 98
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. AWS Classic Load Balancer
D. Amazon Route 53

Answer: A
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html
correct https://aws.amazon.com/elasticloadbalancing/features/ , ALB supports path based
https://aws.amazon.com/elasticloadbalancing/features/?nc=sn&loc=2 ALB - Load Balancing to multiple ports on the same instance

Path based routing= Application Load Balancer

QUESTION 99

A data analytics startup company asks a Solutions Architect to recommend an AWS data store option 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 models 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
The correct answer is C and the key here is "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".

QUESTION 100

A Solutions Architect needs to allow developers to have SSH connectivity to web servers. The requirements are as follows:

- **A. Limit access to users origination from the corporate network.**
- **B. Web servers cannot have SSH access directly from the Internet.**
- **C. Web servers reside in a private subnet.**

Which combination of steps must the Architect complete to meet these requirements? (Choose two.)

A. Create a bastion host that authenticates users against the corporate directory.
B. Create a bastion host with security group rules that only allow traffic from the corporate network.
C. Attach an IAM role to the bastion host with relevant permissions.
D. Configure the web servers' security group to allow SSH traffic from a bastion host.
E. Deny all SSH traffic from the corporate network in the inbound network ACL.

Answer: BD
What is Bastion

A **bastion host** is a **server** whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a **bastion host** must minimize the chances of penetration. For example, you can **use** a **bastion host** to mitigate the risk of allowing SSH

https://aws.amazon.com/blogs/security/tag/bastion-host/

https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/

B and D. Bastion host allows corporate dc IPs only, EC2s get traffic from BH SG. It's a very typical setup.

let me elaborate more on this.

First we need to create Bastion host on web subnet which needs to be accessed from corporate network and not from corporate directory. so first part "B" is correct. Then we need to Configure the web servers' security group to allow SSH traffic from a bastion host.
web servers cannot have SSH directly from internet ... so D is needed

Why it is not:

A - Limit access based on corporate 'network' not directory(developers can still use their credentials and login from anywhere on the internet)

C - IAM role not required for this scenario

E - Inbound traffic from corporate network should be allowed, just not directly (hence we are using bastion host)

QUESTION 101
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

What is pilot light disaster recovery AWS?
Regularly test the **recovery** of this **data** and the restoration of your system. **Pilot Light** for Quick **Recovery** into **AWS**. The term **pilot light** is often used to describe a DR scenario in which a minimal version of an environment is always running in the cloud.
https://d1.awsstatic.com/whitepapers/aws-disaster-recovery.pdf
AWS provides a set of cloud-based disaster recovery services that enable fast recovery of your IT infrastructure and data.
https://aws.amazon.com/disaster-recovery/

The database needs the latest data and besides that it might have loads of data which would make it impossible to migrate instantly or within a few minutes. **With cloud formation within a few minutes you have all web servers up and running which is acceptable for a pilot light DR** hence option A is the valid answer.

https://aws.amazon.com/blogs/publicsector/rapidly-recover-mission-critical-systems-in-a-disaster/ Pilot Light
– The idea of the pilot light is an analogy that comes from gas heating. In that scenario, a small flame that's always on can quickly ignite the entire furnace to heat up a house. In this DR approach, you simply replicate part of your IT structure for a limited set of core services so that the AWS cloud environment seamlessly takes over in the event of a disaster. A small part of your infrastructure is always running simultaneously syncing mutable data (as databases or documents), while other parts of your infrastructure are switched off and used only during testing. Unlike a backup and recovery approach, you must ensure that your most critical core elements are already configured and running in AWS (the pilot light). When the time comes for recovery, you can rapidly provision a full-scale production environment around the critical core. With Cloudformation you can build your template with the minimum requirements need to build a 'pilot-light' DR scenario.

https://medium.com/tensult/disaster-recovery-2dd15bea9d39
Here is a diagram depicting how a pilot light DR scenario would look in AWS. http://www.hararei.com/aws-dr-pilot-light.php

QUESTION 102
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

Answer is B. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html#CHAP_Storage.Other.Factors As Read replica isnt in the answers it has to be B

QUESTION 103
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

custom watch metrics for memory and cpu utilization

You can use the CloudWatch agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers. The agent supports both Windows Server and Linux, and ****enables you to select the metrics to be collected****

The reason it is Custom and not Default is because we still need to install CloudWatch Agent. See:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html

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

https://tecadmin.net/monitor-memory-disk-metrics-ec2-linux/

QUESTION 104
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
Checked this document about RDS multi AZ deployment. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). I think the keywords here are "replicates the data to a standby instance in A different Availability Zone (AZ)" That indicate the multi AZ deployment on RDS is not replicate instances into 3 AZs.
https://aws.amazon.com/rds/details/multi-az/
by default Aurora will deploy in atleast three AZ'z and will generate two copies of data in each AZ

QUESTION 105
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

because it asks for the simpliest method. Writing a lambda code will take time while versioning is a default AWS setting

versioning is a prerequisite but MFA is not as you will see below that Amazon says "you can also enable MFA rather than you must also enable MFA". "...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."

https://aws.amazon.com/blogs/aws/new-cross-region-replication-for-amazon-s3/

QUESTION 106

An organization has a long-running image processing application that runs on Spot Instances that will be terminated when interrupted. A highly available workload must be designed to respond to Spot Instance interruption notices. The solution must include a two-minute warning when there is not enough capacity.

How can these requirements be met?

A. Use Amazon CloudWatch Events to invoke an AWS Lambda function that can launch On-Demand Instances.
B. Regularly store data from the application on Amazon DynamoDB. Increase the maximum number of instances in the AWS Auto Scaling group.
C. Manually place a bid for additional Spot Instances at a higher price in the same AWS Region and Availability Zone.
D. Ensure that the Amazon Machine Image associated with the application has the latest configurations for the launch configuration.

Answer: A

"must include a two-minute warning" => Need CloudWatch. Use Amazon CloudWatch Events to invoke an AWS Lambda function that can launch On-Demand Instances.

https://aws.amazon.com/blogs/compute/running-high-scale-web-on-spot-instances/

https://aws.amazon.com/blogs/compute/taking-advantage-of-amazon-ec2-spot-instance-interruption-notices/

https://d2908q01vomqb2.cloudfront.net/1b6453892473a467d07372d45eb05abc2031647a/2018/10/02/appnext-arch-final-drawing.png

QUESTION 107

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 is B since Read replicas in Amazon RDS for MySQL, MariaDB, PostgreSQL, and Oracle are implemented using those engines' native asynchronous replication.

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.

QUESTION 108

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

First we need to understand Environment is Active-Active or Active-Passive? The question shows it is Active-Active Environment because two locations are serving the contents but with latency and both are health. nothing is down or on standby mode. So the correct Answer is "A" with Active-Active failover with latency option.

For an active-active system, Geolocation, Geoproximity, Latency, Multivalue, or Weighted policies would work.

https://medium.com/dazn-tech/how-to-implement-the-perfect-failover-strategy-using-amazon-route53-1cc4b19fa9c7

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

QUESTION 109

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

What is Docker?

Docker is a software platform that allows you to build, test, and deploy applications quickly. ... Running **Docker** on **AWS** provides developers and admins a highly reliable, low-cost way to build, ship, and run distributed applications at any scale.

https://aws.amazon.com/docker/

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html

if you see any word like docker, container, microservices, pods; choose ECS (elastic container service) as the answer. but in the real life, choose Kubernetes for your need.

QUESTION 110

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

Should be A because cloudfront is performance and you need a portal to receive clients requests. API gtw receives the requests and send to lambda with interact with a DB if it is necessary. Both API and Lambda scale automatically and are serverless.

https://www.contino.io/insights/5-killer-use-cases-for-aws-lambda

https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html

https://aws.amazon.com/api-gateway/

Why? once development project is completed , they will use Amazon API-- AWS Lambda is an event-driven, serverless computing platform provided by Amazon as a part of the Amazon Web Services. It is a computing service that runs code in response to events and automatically manages the computing resources required by that code. Amazon API Gateway is an Amazon Web Services (AWS) service offering that allows a developer to connect non-AWS applications to AWS back-end resources, such as servers or code. Amazon API Gateway allows an AWS customer to increase the overall utility of Amazon's other cloud services 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

The web frontend can send requests to Lambda functions via API Gateway HTTPS endpoints. Lambda can handle the application logic. And it is a serverless architecture.

QUESTION 111

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

highly available = multiA-Z

Multi AZ is for failover vs Read Replica purely for reducing the latency, throughput, etc., and there will be small downtime trying to failover from a Read Replica. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

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

because you dont have automatic fail over for Read Replica. Manual intervention is required to point the read replica. Multi AZ has auto fail over if primary database is not reachable for any reason.

QUESTION 112

An organization designs a mobile application for their customers to upload photos to a site. The application needs a secure login with MFA. The organization wants to limit the initial build time and maintenance of the solution.

Which solution should a Solutions Architect recommend to meet the requirements?

A. Use Amazon Cognito Identity with SMS-based MFA.
B. Edit AWS IAM policies to require MFA for all users.
C. Federate IAM against corporate AD that requires MFA.
D. Use Amazon API Gateway and require SSE for photos.

Answer: A

With Amazon Cognito, your users can sign in through social identity providers such as Google, Facebook, and Amazon, and through enterprise identity providers such as Microsoft Active Directory via SAML. https://aws.amazon.com/cognito/

What is MFA
https://aws.amazon.com/iam/features/mfa/

AWS will soon end support for SMS multi-factor authentication (MFA). We are not allowing new customers to preview this feature. We recommend that existing customers switch to one of the following alternative methods of MFA: A virtual (software-based) MFA device A U2F security key A hardware-based MFA device Tip You can view users in your account with an assigned SMS MFA device. In the IAM console, choose Users from the navigation pane, and look for users with SMS in the MFA column of the table.
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_sms.html##targetText=An%20SMS%20(short%20message%20service,used%20only%20with%20IAM%20users.

QUESTION 113
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

Based on this in the question... "data retrieval must occur with minimal latency" -->> DynamoDB is a NoSQL database which is built for high throughput and low latency.

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

erformance at scale DynamoDB supports some of the world's largest scale applications by providing consistent, single-digit millisecond response times at any scale. You can build applications with virtually unlimited throughput and storage.

https://medium.com/swlh/building-dynamodb-brick-by-brick-237e0008b698

QUESTION 114
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 serve static files

Answer: A

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html
What is CloudFront
https://en.wikipedia.org/wiki/Amazon_CloudFront

QUESTION 115
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

redshift is a warehouse solution and also used for analytics: AGgregate keyword

For analyzing 10TB of sales data (structured), we need a DWH solution as Amazon Redshift

1PB is 1000TB

QUESTION 116

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

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).

1. AZ with more instances
2. Oldest launch conf
3. closest to next billing hour
4. if next billing hours matches more than one - then Random termination

QUESTION 117

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 serve 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 serve 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

best choice is A since it is event trigger. this is the Amazon issue, which asks question may have more than answers.
API Gateway can be integrated with HTTP endpoints using HTTP proxy:
https://docs.aws.amazon.com/apigateway/latest/developerguide/setup-http-integrations.html

Whynot B?

API Gateway support unencrypted (HTTP) endpoints in two ways: 1. HTTP Custom Integration or 2.using HTTP proxy
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-create-api-step-by-step.html
https://docs.aws.amazon.com/apigateway/latest/developerguide/setup-http-integrations.html

hence, **option B will work with more cost and more difficult steps**

QUESTION 118
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

they need a relational DB in AWS so answer is A. This is a relational storage system while keeping the cost low.

A. Amazon RDS -> Relational
B. B. Amazon RedShift -> Data warehouse
C. C. Amazon DynamoDB Accelerator ->
D. Non Relational + Performance
E. D. Amazon ElastiCache -> Performance

QUESTION 119
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

It's more cost effective then using other services (redshift).
the question mentions that the solution must be easy to maintain so **A** is not a option, it more involved.

https://itnext.io/getting-started-with-postgresql-using-amazon-rds-cloudformation-pgadmin-and-python-d11aa98e6409 Using the Read Replica: For better application performance, it may be optimal to redirect some or all of the database reads to the read replica, while leaving writes, updates, and deletes to hit the master instance. The script can be easily modified to execute the same query against the read replica rather than the master RDS instance by merely passing the desired section, 'replica' versus 'master', in the call to the set_connection(section) function.

QUESTION 120
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: AC

The question asks to "store this data in a data warehouse to run aggregations and visualizations." . Redshift is datawarehouse application and the answer is A and C.

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

QUESTION 121

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

https://aws.amazon.com/blogs/aws/cross-region-snapshot-copy-for-amazon-rds/
You can copy snapshots of any size, from any of the database engines (MySQL, Oracle, or SQL Server) that are supported by RDS

Why not A ?
Because a read replica is not a point in time copy.

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/

QUESTION 122

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

dynamic= unknown time and date

The question states , random change.. No specific date and time too - Dynamic When you configure dynamic scaling, you define how to scale the capacity of your Auto Scaling group in response to changing demand.

Dynamic https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html

QUESTION 123

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

keyword.: the lowest price per 1TB of data stored , with lead times well in advance of when archived data must be recovered"

Amazon Glacier.: Customers can store data for as little as $1 per terabyte per month

Source: https://aws.amazon.com/glacier/?nc1=h_ls

https://aws.amazon.com/s3/faqs/?nc=sn&loc=7

https://aws.amazon.com/s3/

QUESTION 124

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

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 results.

https://aws.amazon.com/blogs/big-data/writing-sql-on-streaming-data-with-amazon-kinesis-analytics-part-1/

QUESTION 125

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
stream of large-volume. kinesis also using SQL query.
Kinesis Data Analytics
https://docs.aws.amazon.com/kinesisanalytics/latest/dev/how-it-works.html

QUESTION 126
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: BC
You can change the behavior so that Amazon EC2 stops Spot Instances when they are interrupted if the following requirements are met. For a Spot Instance request, the type must be persistent. You cannot specify a launch group in the Spot Instance request. For an EC2 Fleet or Spot Fleet request, the type must be maintain. The root volume must be an EBS volume, not an instance store volume.

EC2 always be EBS volume
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html#interruption-behavior

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html#interruption-behavior
explanation: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html
https://aws.amazon.com/about-aws/whats-new/2017/09/amazon-ec2-spot-can-now-stop-and-start-your-spot-instances/

QUESTION 127
An application hosted on AWS uses object storage for storing internal reports that are accessed daily by the CFO. Currently, these reports are publicly available.

How should a Solutions Architect re-design this architecture to prevent unauthorized access to these reports?

A. Encrypt the files on the client side and store the files on Amazon Glacier, then decrypt the reports on the client side.
B. Move the files to Amazon ElastiCache and provide a username and password for downloading the reports.
C. Specify the use of AWS KMS server-side encryption at the time of an object creation on Amazon S3.
D. Store the files on Amazon S3 and use the application to generate S3 pre-signed URLs to users.

Answer: D
CFO can still access it daily. It just that with the new design if others need access they get do so via pre-signed URL.

KMS has nothing to do with file read access/permissions. KMS is about encryption at rest. on top of that Encryption will encrypt data at rest but will not stop unauthorized access to the bucket. so not C

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

"presigned URLs are valid only for the specified duration." Does this limit the access in any way?
https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html

QUESTION 128

A Solutions Architect is designing an application on AWS that will connect to the on-premise data center through a VPN connection. The solution must be able to log network traffic over the VPN.

Which service logs this network traffic?

A. AWS CloudTrail logs
B. Amazon VPC flow logs
C. Amazon S3 bucket logs
D. Amazon CloudWatch Logs

Answer: B

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 or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

- Flow logs can help you with a number of tasks, such as:
- Diagnosing overly restrictive security group rules
- Monitoring the traffic that is reaching your instance
- Determining the direction of the traffic to and from the network interfaces

Cloudwatch can only show the number of bytes in Tunnel in and out but not the network traffic down to package/request details

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

QUESTION 129

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

Beside strong the data, the question is also requiring accessing data with small latency as well as the cost is not a factor. So DynamoDB is best fit

Dynamo DB : The maximum item size in DynamoDB is 400 KB with milli second latency

The reason why I didn't select B is for EBS HDD is more like storing large sequential data.

QUESTION 130

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

Because S3 Standard IA has best Retrial time than the rest

https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html#sc-infreq-data-access

For example, you might choose the STANDARD_IA and ONEZONE_IA storage classes: For storing backups. For older data that is accessed infrequently, but that still requires millisecond access. For example, when you upload data, you might choose the STANDARD storage class, and use lifecycle configuration to tell Amazon S3 to transition the objects to the STANDARD_IA or ONEZONE_IA class.

https://aws.amazon.com/s3/storage-classes/

B. Amazon Glacier standard retrievals typically retrieval within 3 – 5 hours

C. Amazon Glacier bulk retrievals: retrievals typically complete within 5 – 12 hours

D. Amazon S3 Standard Infrequent Access - Best fit Answer

Glacier SLA for data retrieval is more than 2 hours.

https://aws.amazon.com/blogs/aws/aws-storage-update-s3-glacier-price-reductions/

QUESTION 131

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

if its a "performance" issue, then read replicas

RDS Read Replicas for reads(SELECT statements) scalability.

RDS Multi-AZ (Disaster Recovery) hence Increase availability

https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-Lab2cjLoX9c9IgJaCN8/Please%20assist%20me%20in%20a%20practice%20problem,%20I%20have%20included%20my%20reasoning%20and%20the%20solution

QUESTION 132

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

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

Dynamodb, Lambda and S3 are already high available. Only option not being, is RDS.

"Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments"

"A" - S3 already has the highest availability between all services

"B" - Lambda already deployed in multiple AZ and Regions
"C" - has limited (vertical) scalability, is not deployed in M-AZ "
D" - already has high availability (5 nines)

QUESTION 133
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
Standard Glacier is 3-5 hours and the Bulk Retrieval is 5-12 hours
Deep Archive Glacier is 12 hours
https://aws.amazon.com/s3/storage-classes/
https://aws.amazon.com/glacier/faqs/

https://aws.amazon.com/about-aws/whats-new/2016/11/access-your-amazon-glacier-data-in-minutes-with-new-retrieval-options/

QUESTION 134
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
https://aws.amazon.com/blogs/database/automating-sql-caching-for-amazon-elasticache-and-amazon-rds/

1. the requirement is "improve the performance"
2. 2. the issue was due to "SAME complex database queries were causing increased latency" this can be done through using Amazon ElastiCache

QUESTION 135
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
https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html
AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.
An AWS *resource* is an entity you can work with in AWS, such as an Amazon Elastic Compute Cloud (EC2) instance, an Amazon Elastic Block Store (EBS) volume, a security group, or an Amazon Virtual Private Cloud (VPC). For a complete list of AWS resources supported by AWS Config, see AWS Config Supported Resource Types and Resource Relationships.
With AWS Config, you can do the following:

- Evaluate your AWS resource configurations for desired settings.

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

QUESTION 136
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

You can encrypt your Amazon RDS DB instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instances. Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, read replicas, and snapshots.

Amazon RDS encrypted DB instances use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS DB instances. After your data is encrypted, Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance. You don't need to modify your database client applications to use encryption.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

QUESTION 137
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
Dynamo DB streams to trigger a Lambda function https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html

QUESTION 138
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

SSE-S3

Protecting Data Using Server-Side Encryption with Amazon **S3**-Managed Encryption Keys (**SSE**-**S3**) ...
Amazon **S3** encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly.

Server-side encryption protects data at rest. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available to encrypt your data, 256-bit Advanced Encryption Standard (AES-256).

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

SSE-**S3** requires that Amazon **S3** manage the data and master encryption keys. For more information about **SSE**-**S3**, see Protecting Data Using Server-Side Encryption with Amazon **S3**-Managed Encryption Keys (**SSE**-**S3**). ... **SSE**-**KMS** requires that AWS manage the data key but you manage the customer master key (CMK) in AWS **KMS**.

SSE-KMS https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

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

QUESTION 139
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

https://aws.amazon.com/blogs/big-data/encrypt-your-amazon-redshift-loads-with-amazon-s3-and-aws-kms/

https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html

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

QUESTION 140
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

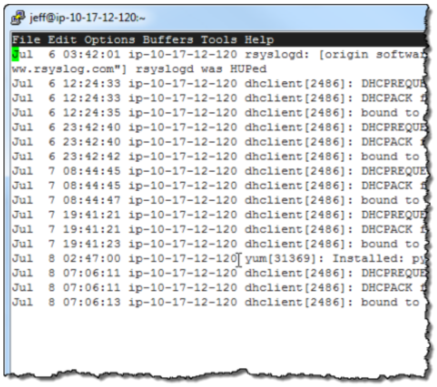
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html

The logs collected by the unified CloudWatch agent are processed and stored in Amazon CloudWatch Logs, just like logs collected by the older CloudWatch Logs agent.

Use an Amazon CloudWatch agent to push the logs to Amazon CloudWatch Logs.
https://aws.amazon.com/blogs/aws/cloudwatch-log-service/

Amazon introducing a powerful new log storage and monitoring feature for **Amazon CloudWatch.** You can now route your operating system, application, and custom log files to CloudWatch, where they will be stored in durable fashion for as long as you'd like. You can also configure CloudWatch to monitor the incoming log entries for any desired symbols or messages and to surface the results as CloudWatch metrics. You could, for example, monitor your web server's log files for 404 errors to detect bad inbound links or 503 errors to detect a possible overload condition. You could monitor your Linux server log files to detect resource depletion issues such as a lack of swap space or file descriptors. You can even use the metrics to raise alarms or to initiate Auto Scaling activities.

Here are some new terms that you will need to understand in order to use CloudWatch to store and monitor your logs:



```
Jul  6 03:42:01 ip-10-17-12-120 rsyslogd: [origin softwa
ww.rsyslog.com"] rsyslogd was HUPed
Jul  6 12:24:33 ip-10-17-12-120 dhclient[2486]: DHCPREQUE
Jul  6 12:24:33 ip-10-17-12-120 dhclient[2486]: DHCPACK f
Jul  6 12:24:35 ip-10-17-12-120 dhclient[2486]: bound to
Jul  6 23:42:40 ip-10-17-12-120 dhclient[2486]: DHCPREQUE
Jul  6 23:42:40 ip-10-17-12-120 dhclient[2486]: DHCPACK f
Jul  6 23:42:42 ip-10-17-12-120 dhclient[2486]: bound to
Jul  7 08:44:45 ip-10-17-12-120 dhclient[2486]: DHCPREQUE
Jul  7 08:44:45 ip-10-17-12-120 dhclient[2486]: DHCPACK f
Jul  7 08:44:47 ip-10-17-12-120 dhclient[2486]: bound to
Jul  7 19:41:21 ip-10-17-12-120 dhclient[2486]: DHCPREQUE
Jul  7 19:41:21 ip-10-17-12-120 dhclient[2486]: DHCPACK f
Jul  7 19:41:23 ip-10-17-12-120 dhclient[2486]: bound to
Jul  8 02:47:00 ip-10-17-12-120 yum[31369]: Installed: py
Jul  8 07:06:11 ip-10-17-12-120 dhclient[2486]: DHCPREQUE
Jul  8 07:06:11 ip-10-17-12-120 dhclient[2486]: DHCPACK f
Jul  8 07:06:13 ip-10-17-12-120 dhclient[2486]: bound to
```

- Log Event – A Log Event is an activity recorded by the application or resource being monitored. It contains a timestamp and raw message data in UTF-8 form.
- Log Stream – A Log Stream is a sequence of Log Events from the same source (a particular application instance or resource).
- Log Group – A Log Group is a group of Log Streams that share the same properties, policies, and access controls.
- Metric Filters – The Metric Filters tell CloudWatch how to extract metric observations from ingested events and turn them in to CloudWatch metrics.
- Retention Policies – The Retention Policies determine how long events are retained. Policies are assigned to Log Groups and apply to all of the Log Streams in the group.
- Log Agent – You can install CloudWatch Log Agents on your EC2 instances and direct them to store Log Events in CloudWatch. The Agent has been tested on the Amazon Linux AMIs and the Ubuntu AMIs. If you are running Microsoft Windows, you can configure the ec2config service on your instance to send systems logs to CloudWatch. To learn more about this option, read the documentation on Configuring a Windows Instance Using the EC2Config

QUESTION 141

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: CD

"C" - to ensure the order "D" - the question clearly says - "likely have high usage spikes", that means that our solution has to be elastic, and the only one elastic option in the list of possible answers is "D"

QUESTION 142

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

1)it is an application(Not website). 2)
Question is how you handle the traffic? that means we already few instance in place with ELB. however they are not able to handle the traffic . so we are introducing the Auto scaling to scale the instance based on the traffic.

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

https://aws.amazon.com/ec2/autoscaling/

for example (Thanksgiving sales)

if you facing a spike traffic , that means the amount of servers active and actually configured to handle the demand are overload,. so even if you use a Route 53 latency routing policy to route traffic to existing ec2 on your configuration that will no add performance, course routing policy here is to redirect traffic to least ec2 lag time. we need more servess or a more powerful server to resolve this issue.

QUESTION 143

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

FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated. The order in which messages are sent and received is strictly preserved and a message is delivered once and remains available until a consumer processes and deletes it

https://aws.amazon.com/about-aws/whats-new/2019/02/amazon-sqs-fifo-qeues-now-available-in-15-aws-regions/

Q: Does Amazon SQS provide message ordering? "

Yes. FIFO (first-in-first-out) queues preserve the exact order in which messages are sent and received. If you use a FIFO queue, you don't have to place sequencing information in your messages. For more information, see FIFO Queue Logic in the Amazon SQS Developer Guide. Standard queues provide a loose-FIFO capability that attempts to preserve the order of messages. However, because standard queues are designed to be massively scalable using a highly distributed architecture, receiving messages in the exact order they are sent is not guaranteed." https://aws.amazon.com/sqs/faqs/

QUESTION 144

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
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

Lack of information to pick the *best* solution for the scenario. The answer should be Route 53. There are OPTIONS inside R53, which would fit (latency, geolocation and geoproximity are 3 valid solutions inside R53). A is incorrect because the content is dynamic, although AWS loves to say that CloudFront can cache dynamic content, it's not 100% true (CloudFront can cache static content, and SOME dynamic content such as ZIP code, for example)

cloudfront has a geo-restriction not a geo routing ans is B https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/

QUESTION 145

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

Answer D provide most scalable solution. https://aws.amazon.com/blogs/gametech/tag/aws-lambda/

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/

read case study here https://aws.amazon.com/blogs/gametech/game-developers-guide-to-the-aws-sdk/

QUESTION 146

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
Nat == connecting the internet

QUESTION 147

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

S3 and S3-IA has the same retrieval time. The diff is that you are charged for retrieval. Availability is 99.99 vs 99.9. They want also the most COST-effective solution. Glacier is in minutes so not instantly.

QUESTION 148
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

use SQS queue, most cost effective solution

https://www.pgs-soft.com/blog/how-to-build-run-a-high-performance-serverless-voting-system-for-less-than-100

QUESTION 149
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: B

A **dead**-**letter queue** is a **queue** that other (source) **queues** can target for messages that can't be processed (consumed) successfully. In this tutorial you learn how to create an Amazon **SQS** source **queue** and to configure a second **queue** as a **dead**-**letter queue** for it.

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-dead-letter-queue.html

QUESTION 150
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

Previously(before Jun 20, 2019), you had to manually provision storage capacity based on anticipated application demands. Under-provisioning could result in application downtime, and over-provisioning could result in underutilized resources and higher costs. With RDS Storage Auto Scaling, you simply set your desired maximum storage limit, and Auto Scaling takes care of the rest.
https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/

QUESTION 151

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 is rarely changed. Clients only access one record at a time.

Database access has been increasing exponentially due to increased client demand. The resultant load will soon exceed the capacity of the most expensive hardware available for purchase. The 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

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/

DynamoDB supports some of the world's largest scale applications by providing consistent, single-digit millisecond response times at any scale. You can build applications with virtually unlimited throughput and storage. DynamoDB global tables replicate your data across multiple AWS Region.
https://aws.amazon.com/dynamodb/

QUESTION 152

A business team requires a structured storage solution to store all of a company's historical sales data. Currently there are 4 TB of data, which will grow to hundreds of terabytes within a few years. The team must be able to regularly run queries against the data using current business intelligence tools. Fast performance is required despite the dataset growth.

Which solution should the company use?

A. Amazon Redshift
B. Amazon Aurora
C. Amazon DynamoDB
D. Amazon S3

Answer: A

keywords:
-hundreds of terabytes –
business intelligence queries –
Fast performance is required despite the dataset growth

Amazon Simple Storage Service (S3) is the largest and most performant object storage service for structured and unstructured data and the storage service of choice to build a data lake. With a data lake built on Amazon S3, you can use native AWS services to run big data analytics, artificial intelligence (AI), machine learning (ML), high-performance computing (HPC) and media data processing applications to gain insights from your unstructured data sets. Amazon S3 hosts tens of thousands of data lakes for household brands such as Netflix, Airbnb, Sysco, Expedia, GE, and FINRA, who are using them to securely scale with their needs and to discover business insights every minute. https://aws.amazon.com/products/storage/data-lake-storage/

QUESTION 153

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

AWS Lambda functions, No specialize Hardware

QUESTION 154

An application that runs on an Amazon EC2 instance must make secure calls to Amazon S3 buckets.

Which steps can a Solutions Architect take to ensure that the calls are made without exposing credentials?

A. **Generate an access key ID and a secret key, and assign an IAM role with least privilege.**
B. **Create an IAM policy granting access to all services and assign it to the Amazon EC2 instance profile.**
C. **Create an IAM role granting least privilege and assign it to the Amazon EC2 instance profile.**
D. **Generate temporary access keys to grant users temporary access to the Amazon EC2 instance.**

Answer: C

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances.
We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows:

1. Create an IAM role.
2. Define which accounts or AWS services can assume the role.
3. Define which API actions and resources the application can use after assuming the role.
4. Specify the role when you launch your instance, or attach the role to an existing instance.
5. Have the application retrieve a set of temporary credentials and use them.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

QUESTION 155

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

You can use the CloudWatch Logs agent installer on an existing EC2 instance to install and configure the CloudWatch Logs agent. After installation is complete, logs automatically flow from the instance to the log stream you create while installing the agent. The agent confirms that it has started and it stays running until you disable it.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html

QUESTION 156

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.

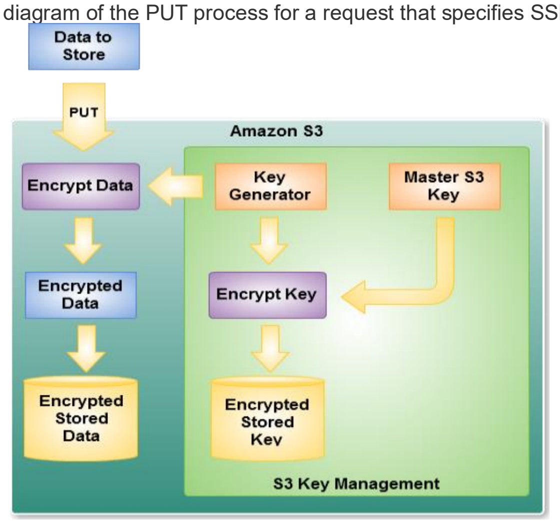
Which of the following answers this question?

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

https://aws.amazon.com/blogs/aws/new-amazon-s3-server-side-encryption/

Amazon S3 Server Side Encryption handles all encryption, decryption, and key management in a totally transparent fashion. When you PUT an object and request encryption (in an HTTP header supplied as part of the PUT), we generate a unique key, encrypt your data with the key, and then encrypt the key with a master key. For added protection, keys are stored in hosts that are separate and distinct from those used to store your data. Here’s a diagram of the PUT process for a request that specifies SSE:



Decryption of the encrypted data requires no effort on your part. When you GET an encrypted object, we fetch and decrypt the key, and then use it to decrypt your data. We also include an extra header in the response to the GET to let you know that the data was stored in encrypted form in Amazon S3.

https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetBucketEncryption.html?shortFooter=true

https://aws.amazon.com/blogs/aws/new-amazon-s3-server-side-encryption/

QUESTION 157

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

DynamoDB - Though its not default, it supports strong consistency read

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

https://aws.amazon.com/blogs/aws/improved-queries-and-updates-for-dynamodb/

QUESTION 158

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

C is 4 Instances in 2 availability Zones = **8 instances** running all time. It fits the Fault tolerance scenario, but not cost.
Answer is A, to have 2 instances running on 3 AZs, meaning paying for **6 instances** and also having Fault Tolerance for the requirement for four instances in 2 separated AZs.

2*3 = 6 EC2 (need to pay for 6) and in C 4*2 =8 EC2 (needs to pay for 8)

every(3) AZ will have two instances,if one AZ is down you will still have four instances running all the time.

https://www.rackspace.com/blog/aws-101-regions-availability-zones

QUESTION 159

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
Security Groups only allow you to 'Allow' traffic, not 'Deny' it (making Answer B not possible):
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Security Group Basics
The following are the basic characteristics of security groups for your VPC:
You can specify allow rules, but not deny rules.

QUESTION 160

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: AD

There is bastion host in A-Cloud Guru AWS Solutions Architect course (065 NATs vs. Bastions): "Bastion hosts allows you to SSH or RDP into the Bastion and then initiate a private connection over private networks to your instances to administer them". To add my contribution to this, A and D are correct because option B would require opening either SSH or RDP ports (or both) on the web servers which should normally only have web HTTP or HTTPS (or both) ports, which to me does not make any sense so A and D are correct for me.

Agreed on A and D largely by process of wrong answer elimination.
B - Bad practise, you wouldn't hop onto a web server just to access another server in a private subnet - this would be a security vulnerability. This is especially true with a Bastion Host answer option being available.
C - NAT Gateways allow servers out to the internet but prevent incoming connections from the internet - completely the opposite of what we are trying to achieve here: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
NAT Gateways You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. For more information about NAT, see NAT.
E - Elastic IPs are public which, if attached to the database, would invalid it from being in a private subnet in the first place

QUESTION 161
A web application running on Amazon EC2 instances writes data synchronously to an Amazon DynamoDB table configured for 60 write capacity units. During normal operation the application writes 50 KB/s to the table, but can scale up to 500 KB/ s during peak hours. The application is currently getting throttling errors from the DynamoDB table during peak hours.

What is the MOST cost-effective 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
Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

QUESTION 162
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

Issue I want to give another AWS account access to an object that is stored in an Amazon Simple Storage Service (Amazon S3) bucket. How can I provide cross-account access to Amazon S3 buckets? In the following example policies, be sure to update the policy to include your relevant account ID, bucket name, ARN, and so on. As per the URL : https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html , Says Account A administrator user attaches a bucket policy granting cross-account permissions to Account B to perform specific bucket operations. Note that administrator user in Account B will automatically inherit the permissions. Account B administrator user attaches user policy to the user delegating the permissions it received from Account A. User in Account B then verifies permissions by accessing an object in the bucket owned by Account A

https://aws.amazon.com/s3/features/#Access_management_and_security

How can I provide cross-account access to objects that are in Amazon S3 buckets?

https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/

Use one of the following methods to grant cross-account access to objects that are stored in S3 buckets:

- Resource-based policies and AWS Identity and Access Management (IAM) policies for programmatic-only access to S3 bucket objects
- Resource-based Access Control List (ACL) and IAM policies for programmatic-only access to S3 bucket objects
- Cross-account IAM roles for programmatic and console access to S3 bucket objects

Bucket Owner Granting Cross-Account Bucket Permissions https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html

QUESTION 163

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

On- Demand instances will not offer the "MOST cost-effective way" solution requirement "A Reserved Instance is an instance rented for a fixed period of time at a lower rate than basic AWS On- Demand instances" https://medium.com/@jaychapel/aws-reserved-instances-versus-on-demand-which-is-better-e7f77f1f9582

so the answer is D 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.zon DynamoDB Auto Scaling to handle the extra demand.

Key in the question here 'must have' and combined with 'most cost efficient'.
Taking the 'always one instance running' criteria, this immediately rules out Answers B and C as these are using on-demand instances which won't be as cheap as a reserved instance - the other information (even including the spot instances on answer C) is largely irrelevant at this point.
This leaves us ruling out A which is fairly straight forward - CPU utilization gives us no guarantee that we will have the 4 instances required and the "to add and remove EC2 instances based on CPU utilization. " statement in the answer also doesn't tell us what type of instances will be added or removed.
Answer D clearly tells us that one reserved instance will be running and a scheduled action to add 3 EC2 On-Demand instances and the correct times will be added - this satisfies the 'must have' and 'cost-efficient' criteria.

QUESTION 164

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
you need to add at least 2 subnets to the ELB to make it HA: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-manage-subnets.html

QUESTION 165
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
The correct answer is "C", here is why others are wrong: "
A" - You cannot distribute traffic by Route 53 to autoscaling groups without creating custom scripts that would update DNS https://aws.amazon.com/blogs/compute/building-a-dynamic-dns-for-route-53-using-cloudwatch-events-and-lambda/
"B" - ELB is a regional service so it cannot distribute traffic between different Regions
"C" - is a way to go
"D" - same as "A"

QUESTION 166
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: B

Elastic Beanstalk is the answer, as Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring, you just have to concentrate on your code.

QUESTION 167
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

https://aws.amazon.com/ec2/dedicated-hosts/

Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2, so that you get the flexibility and cost effectiveness of using your own licenses, but with the resiliency, simplicity and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirements.

QUESTION 168
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

https://aws.amazon.com/efs/

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

QUESTION 169
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

please note the key words, microservice=container=ECS.

Lambda Concurrent Execution default limit 1,000

it mentioned : micro service. A and B is not micro service. only C and D are Micro service. and obviously AMS provide docker directly it is not necessary to use EC2 to install docker.

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

Docker makes it easy to build and run distributed microservices architecures, deploy your code with standardized continuous integration and delivery pipelines, build highly-scalable data processing systems, and create fully-managed platforms for your developers. Docker also provides big data processing as a service. (https://aws.amazon.com/docker/)

QUESTION 170
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
I think this question is really focusing on scaling delay. We're told that the DynamoDB database has a utilisation target to scale at 80% and increase the read/write units by 5. Without any other metrics we would assume this is done instantly / as required and that it is sufficient to satisfy any DB requirements that the EC2 web servers are placing upon it. With answer the EC2 scaling, we are told that "Auto Scaling is currently configured to add a new web server when CPU is greater than 80% for 5 minutes." - I think this is the key. To provide an example, if the load required approximately needed 8 EC2 instances and at 9am when everyone logged in to check their results, there were only 2 EC2 instances running, there would be a 30 minute lag whilst EC2 instances are added 1 at a time at intervals of 5 minutes which would match the observations that the issue disappears by 9:30am. If the scheduled scaling is performed before 9am and taken down after 9:30am, this would satisfy the complaints without costing the earth in the process.

QUESTION 171
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: C
The key difference between **stateful** and **stateless** applications is that **stateless applications don't “store” data** whereas **stateful applications require backing storage**. ... Any associated storage is typically ephemeral. If the container restarts for instance, anything stored is lost

With Amazon Cognito, your users can sign in through social identity providers such as Google, Facebook, and Amazon, and through enterprise identity providers such as Microsoft Active Directory via SAML.

https://aws.amazon.com/cognito/

QUESTION 172

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

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

QUESTION 173

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:

Application must remain available at all times" This will eliminate B (Spot instances can terminate at any time) & D for minimum instances to 0 "A" is not at all to consider meaning less.

QUESTION 174

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

https://dzone.com/articles/confused-by-aws-storage-options-s3-ebs-amp-efs-explained

EFS: $0.30/GB

S3: $0.0245/GB

S3 now provide 3500 maximum request. In additional, it sharing document on web application, not sharing for multiple EC2

MOST Cost -effective Storage solution. Refer this URL: beautiful comparison between S3, EBS, EFS you will bookmark it for sure

https://cloud.netapp.com/blog/ebs-efs-amazons3-best-cloud-storage-system

https://www.apptio.com/emerge/aws-s3-understanding-cloud-storage-costs-to-save/

QUESTION 175

A Solutions Architect was tasked with reviewing several templates that build VPCs and ensuring that they meet specific security requirements. After reviewing the templates, the Architect realizes that all of the templates are missing important security best practices.

What should the Architect do to implement security best practices in an efficient manner?

A. Use VPC peering to enforce network consistency
B. Restrict users from deploying an AWS CloudFormation template
C. Provide the teams a nested AWS CloudFormation template that builds the VPC correctly
D. Create AWS Identity and Access Management (IAM) policies that enforce the corporate VPC architecture standards

Answer: C

Keyword: 'missing important security best practices' You use Cloudformation nested stacks to fill-out the missing security best practices by creating additional dedicated templates and reference them in the existing current templates.

As your infrastructure grows, common patterns can emerge in which you declare the same components in multiple templates. You can separate out these common components and create dedicated templates for them. Then use the resource in your template to reference other templates, creating nested stacks.

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

https://aws.amazon.com/blogs/devops/aws-cloudformation-security-best-practices/

https://docs.aws.amazon.com/quickstart/latest/compliance-nist/templates.html The Quick Start consists of a master template and seven child templates: IAM, logging, production VPC, management VPC, Config rules, NAT instance, and application. These templates are designed to deploy the architecture within stacks that align with AWS best practices and the security compliance framework.

QUESTION 176

A Solutions Architect has been given the following requirements for a company's VPC:

The solution is a two-tiered application with a web tier and a database tier.

- **All web traffic to the environment must be directed from the Internet to an Application Load Balancer.**
- **The web servers and the databases should not obtain public IP addresses or be directly accessible from the public Internet.**
- **Because of security requirements, databases may not share a route table or subnet with any other service.**
- **The environment must be highly available within the same VPC for all services.**

What is the minimum number of subnets that the Solutions Architect will need based on these requirements and best practices?

A. 2
B. 3
C. 4
D. 6

Answer D

2 public subnets for ALB, 2 private subnets for web tier and 2 private subnets for db tier across 2AZ's

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load-balancer-getting-started.html

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

QUESTION 177

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

because the data should be inmediatly available all the time for batch jobs

Keyword " data should be immediately available all the time for batch jobs". As per aws doc, we can move data from S3 to other storage before 30 days but will incur the normal storage usage charge plus a pro-rated request charge for the remainder of the 30-day minimum. https://aws.amazon.com/s3/pricing/

https://aws.amazon.com/s3/storage-classes/ Look at Minimum Storage Duration.

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

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

QUESTION 178

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

Kinesis allows process in order and Each shard can support up to 1000 PUT records per second.

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

SQS FIFO does not allow single message to be processed more than once, which is a requirement here.

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.

QUESTION 179

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

AWS Systems Manager Parameter Store. AWS Systems Manager Parameter Store provides secure, hierarchical storage for configuration data management and secrets management. You can store data such as passwords, database strings, and license codes as parameter values.
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html

AWS Secrets Manager secure your database credentials and send them to Lambda functions that will use them to connect and query the backend database service Amazon RDS—without hardcoding the secrets in code or passing them through environment variables https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by-using-aws-secrets-manager/ https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html

I think the keyword here for not selecting D is "SQL database" Check this document out. You can authenticate to your DB instance using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with MySQL and PostgreSQL.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html#UsingWithRDS.IAMDBAuth.Availability

QUESTION 180

A company has two different types of reporting needs on their 200-GB data warehouse:

- **Data scientists run a small number of concurrent ad hoc SQL queries that can take several minutes each to run.**
- **Display screens throughout the company run many fast SQL queries to populate dashboards.**

Which design would meet these requirements with the LEAST cost?

A. Replicate relevant data between Amazon Redshift and Amazon DynamoDB. Data scientists use Redshift. Dashboards use DynamoDB.
B. Configure auto-replication between Amazon Redshift and Amazon RDS. Data scientists use Redshift. Dashboards use RDS.
C. Use Amazon Redshift for both requirements, with separate query queues configured in workload management.
D. Use Amazon Redshift for Data Scientists. Run automated dashboard queries against Redshift and store the results in Amazon ElastiCache. Dashboards query ElastiCache.

Answer: C

Amazon Redshift workload management (WLM) enables users to flexibly manage priorities within workloads so that short, fast-running queries won't get stuck in queues behind long-running queries.
When you have several users running queries against the database, you might find another configuration to be more efficient. For example, if some users run resource-intensive operations, such as VACUUM, these might have a negative impact on less-intensive queries, such as reports. You might consider adding additional queues and configuring them for different workloads.
https://docs.aws.amazon.com/redshift/latest/dg/c_workload_mngmt_classification.html
Defined in the summary for the cost concern https://aws.amazon.com/blogs/big-data/run-mixed-workloads-with-amazon-redshift-workload-management/

Elastic cache has more cost
Elastic cache - pricing https://aws.amazon.com/elasticache/pricing/

QUESTION 181

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

By default, CloudFront caches a response from Amazon S3 for 24 hours (Default TTL of 86,400 seconds). If your request lands at an edge location that served the Amazon S3 response within 24 hours, CloudFront uses the cached response even if you updated the content in Amazon S3.

You can invalidate an S3 object to remove it from the CloudFront distribution's cache. After the object is removed from the cache, the next request retrieves the object directly from Amazon S3.

https://aws.amazon.com/es/premiumsupport/knowledge-center/cloudfront-serving-outdated-content-s3/

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

QUESTION 182

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: AE
Static data on S3 => improve performance and low-latency
Read Replica => improve performance and low-latency

QUESTION 183

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

dynamoDb can store session data

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

Many of the concepts of NoSQL architectures trace their foundational concepts back to whitepapers published in 2006 and 2007 that described distributed systems like Dynamo at Amazon. Today, many application teams use Hbase, MongoDB, Cassandra, CouchDB, Riak, and Amazon DynamoDB to store large volumes of data with high transaction rates. Many of these database engines support clustering and scale horizontally across many machines for performance and fault tolerance. **A common use case for NoSQL is managing user session state, user profiles, shopping cart data, or time-series data**.

QUESTION 184

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

inbound rule for SG allowing port 80/443

QUESTION 185
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

They want improve in performance and elastic Option C cover it all

A. Disqualified due to manual scaling

B. Close to being selected, but disqualified due to no auto-scaling

C. My choice!

D. Disqualified due to hybrid design. Client wants to migrate to AWS

QUESTION 186
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

Host-based routing routes between domain1.example.com and domain2.example.com. What we need here is path-based routing

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html

https://aws.amazon.com/premiumsupport/knowledge-center/elb-achieve-path-based-routing-alb/

QUESTION 187
A Solutions Architect is asked to improve the fault tolerance of an existing Python application. The web application places 1-MB images in 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

S3 can invoke Lambda directly. Easier. Faster.

https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html

https://dashbird.io/blog/what-are-aws-lambda-triggers/

Three Ways To Trigger Lambda: To trigger a lambda function, you can choose between many different ways. Here are the 3 most common ways.

there are 3 ways to trigger lambda:-

1-API Gateway event

2-DynamoDB events

3- S3 events

QUESTION 188
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

An Origin Access Identity (**OAI**) is used for sharing private content via CloudFront. The **OAI** is a virtual user identity that will be used to give your CF distribution permission to fetch a private object from your origin server (e.g. S3 bucket).

https://docs.rightscale.com/cm/dashboard/clouds/aws/cloudfront_origin_access_identities.html

https://medium.com/@ratulbasak93/serving-private-content-of-s3-through-cloudfront-signed-url-593ede788d0d

https://aws.amazon.com/blogs/developer/accessing-private-content-in-amazon-cloudfront/

https://docs.rightscale.com/cm/dashboard/clouds/aws/cloudfront_origin_access_identities.html

QUESTION 189
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

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

There is no additional charge for Elastic Beanstalk - you pay only for the AWS resources needed to store and run your applications.

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

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

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

QUESTION 190

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

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

A *network access control list (ACL)* is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. For more information about the differences between security groups and network ACLs, see Comparison of security groups and network ACLs.

http://chopmo.dk/posts/2015/06/13/blocking-traffic-in-aws.html

Allow or Deny rules Security group support allow rules only (by default all rules are denied). e.g. You cannot deny a certain IP address from establishing a connection.

Network ACL support allow and deny rules. By deny rules, you could explicitly deny a certain IP address to establish a connection example: Block IP address 123.201.57.39 from establishing a connection to an EC2 Instance.

https://medium.com/awesome-cloud/aws-difference-between-security-groups-and-network-acls-adc632ea29ae

Why not WAF

WAF --cost associated ..NACL is free

https://docs.aws.amazon.com/waf/latest/developerguide/tutorials-common-attacks.html

You can't use WAF, if you are NOT using API Gateway, Amazon CloudFront or an Application Load Balancer components. So the answer is B.

https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

QUESTION 191

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

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

It is possible to store several data versions and manage their lifecycle in S3. Upon expiration, data is deleted or it can be transferred to S3 Glacier. If you set a storage class equal to 0 days, information will be immediately sent to S3 Glacier. It is of use when information is rarely accessed in everyday life but its storage life is limited. Though, it might seem that uploading data to S3 first and go with it to Glacier afterward might be more expensive, AWS has ensured that this exact scenario leads to no more expenses than direct Glacier upload.

QUESTION 192

A web application runs on 10 EC2 instances launched from a single customer Amazon Machine Image (AMI). The EC2 instances are behind an Internet Application Load Balancer. Amazon Route 53 provides DNS for the application.

How should a Solutions Architect automate recovery when a web server instance stops replying to request?

A. Launch the instances in an Auto Scaling group with an Elastic Load Balancing health check.

B. Launch instances in multiple Availability Zones and set the load balancer to Multi-AZ.

C. Add CloudWatch alarm actions for each instance to restart if the Status Check (Any) fails.

D. Add Route 53 records for each instance with an instance health check.

Answer : A

ALB triggers rolling out of new instance if instance fails to pass health check

Please check this URL https://aws.amazon.com/premiumsupport/knowledge-center/automatic-recovery-ec2-cloudwatch/

Especially the Note: The CloudWatch recovery option works only for system check failures, not for instance status check failures. In addition, if you terminate your instance, then it can't be recovered.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-elb-healthcheck.html If you attached one or more load balancers or target groups to your Auto Scaling group, the group does not, by default, consider an instance unhealthy and replace it if it fails the load balancer health checks. However, you can optionally configure the Auto Scaling group to use Elastic Load Balancing health checks. This ensures that the group can determine an instance's health based on additional tests provided by the load balancer. The load balancer periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called health checks.

QUESTION 193

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

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

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second. DAX does all the heavy lifting required to add in-memory acceleration to your DynamoDB tables, without requiring developers to manage cache invalidation, data population, or cluster management. Now you can focus on building great applications for your customers without worrying about performance at scale. You do not need to modify application logic, since DAX is compatible with existing DynamoDB API calls. You can enable DAX with just a few clicks in the AWS Management Console or using the AWS SDK. Just as with DynamoDB, you only pay for the capacity you provision. Learn more about DAX pricing on the pricing page.

Elasticache is for RDS Read

what the questions says in the begining. DAX is DynamoDB's in memory cache "retrieves data for customers from a DynamoDB table"

QUESTION 194
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
C is less operational and in time of administrative effort compare to B...

QUESTION 195
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
https://aws.amazon.com/about-aws/whats-new/2016/09/reader-end-point-for-amazon-aurora/

the reader endpoint to provide high availability for your read-only queries from your DB cluster by placing multiple Aurora Replicas in different Availability Zones and then connecting to the read-only endpoint for your read workload. The reader endpoint also load-balances connections to the Aurora Replicas in a DB cluster.

Using the Reader Endpoint You use the reader endpoint for read-only connections for your Aurora cluster. This endpoint uses a load-balancing mechanism to help your cluster handle a query-intensive workload. The reader endpoint is the endpoint that you supply to applications that do reporting or other read-only operations on the cluster. The reader endpoint only load-balances connections to available Aurora Replicas in an Aurora DB cluster. It doesn't load-balance individual queries. If you want to load-balance each query to distribute the read workload for a DB cluster, open a new connection to the reader endpoint for each query. Each Aurora cluster has a single built-in reader endpoint, whose name and other attributes are managed by Aurora. You can't create, delete, or modify this kind of endpoint.

QUESTION 196
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
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html
Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

- If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.
- If the content is not in that edge location, CloudFront retrieves it from an origin that you've defined—such as an Amazon S3 bucket, a MediaPackage channel, or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.

QUESTION 197
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:

One of the goals of moving this application to AWS is to increase the reliability of the storage tier

QUESTION 198
A Solutions Architect is designing a two-tier application for maximum security, with a web tier running on EC2 instances and the data stored in an RDS DB instance. The web tier should accept user access only through HTTPS connections (port 443) from the Internet, and the data must be encrypted in transit to and from the database.

What combination of steps will MOST securely meet the stated requirements? (Choose two.)

A. Create a security group for the web tier instances that allows inbound traffic only over port 443.
B. Enforce Transparent Data Encryption (TDE) on the RDS database.
C. Create a network ACL that allows inbound traffic only over port 443.

D. Configure the web servers to communicate with RDS by using SSL, and issue certificates to the web tier EC2 instances.

E. Create a customer master key in AWS KMS and apply it to encrypt the RDS instance.

Answer: AD
NACL and SGroups are in the same "security level". Since the communication is from the web servers to the DBs, we are talking about SGs. A

QUESTION 199
A credit card processing application, hosted on an on-premises server, needs to communicate directly with a database hosted on an Amazon EC2 instance running in a private subnet of a VPC. Compliance requirements state that end-to-end communication should be encrypted.

Which solution will ensure that this requirement is met?

A. Use HTTPS for traffic over VPC peering between the VPC and the on-premises datacenter.

B. Use HTTPS for traffic over the Internet between the on-premises server and the Amazon EC2 instance.

C. Use HTTPS for traffic over a VPN connection between the VPC and the on-premises datacenter.

D. Use HTTPS for traffic over gateway VPC endpoints that have been configured for the Amazon EC2 instance.

Answer : C

communications are encrypted and secured simply by using a VPN

QUESTION 200
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 ?

A. AWS KMS

B. HTTPS

C. SFTP

D. FTPS

Answer: B

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.

https://searchcloudsecurity.techtarget.com/tip/Amazon-S3-encryption-overview-How-to-secure-data-in-the-Amazon-cloud

Analyzing Amazon S3 encryption

Encrypting data in the cloud means understanding that data can be in one of two states: in transit and at rest. First, to encrypt the transport session used to send and receive data within an Amazon environment, S3 enables users to connect via the HTTPS protocol. This is a fairly standard option among cloud providers, all of whom need to allow SSL-based connectivity to protect sensitive data in transit.

Using KMS is to encrypt at rest, not in transit. ref https://aws.amazon.com/blogs/security/how-to-use-the-rest-api-to-encrypt-s3-objects-by-using-aws-kms/

QUESTION 201
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

QUESTION 202
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

https://aws.amazon.com/getting-started/tutorials/deliver-content-faster/

QUESTION 203
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

QUESTION 204
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

QUESTION 205

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

EBS does not terminate disks on reboots. Instance store does. Actually, the only benefit of the instance store is the speed due to the disk being "closer" to the server, but few companies use that.

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

http://jayendrapatil.com/tag/i2/

QUESTION 206

An organization is deploying Amazon ElastiCache for Redis and requires password protection to improve their data security posture.

Which solution should a Solutions Architect recommend?

A. Redis Auth
B. AWS Single Sign-On
C. IAM database authentication
D. VPC security group for Redis

Answer: A

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

"Using Redis AUTH command can improve data security by requiring the user to enter a password before they are granted permission to execute Redis commands on a password-protected Redis server"

QUESTION 207

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: AD

QUESTION 208
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

QUESTION 209
An application running on Amazon EC2 has been experiencing performance issues when accessing an Amazon RDS for Oracle database. The database has been provisioned correctly for average workloads, but there are several usage spikes each day that have saturated the database, causing the application to time out. The application is write-heavy, updating information more often than reading information. A Solutions Architect has been asked to review the application design.

What should the Solutions Architect recommend to improve performance?

A. **Put an Amazon ElastiCache cluster in front of the database and use lazy loading to limit database access during peak periods.**
B. **Put an Amazon Elasticsearch domain in front of the database and use a Write-Through cache to reduce database access during peak periods.**
C. **Configure an Amazon RDS Auto Scaling group to automatically scale the RDS instance during load spikes.**
D. **Change the Amazon RDS instance storage type from General Purpose SSD to Provisioned IOPS SSD.**

Answer: D

QUESTION 210
During performance testing of an application, the Amazon RDS database caused a performance bottleneck.

What steps can be taken to improve the database performance? (Choose two.)

A. **Change the RDS database instance to multiple Availability Zones.**
B. **Scale up to a larger RDS instance type.**
C. **Redirect read queries to RDS read replicas.**
D. **Scale out using an Auto Scaling group for RDS.**
E. **Use RDS in a separate AWS Region.**

Answer: BC
Usually performance issues of a DB are due to a large number of read requests. So in this case its enough to use a read replica and increase the instance type.

QUESTION 211
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: CE

Because as per AWS TTL is "Time To Live (TTL) for DynamoDB allows you to define when items in a table expire so that they can be automatically deleted from the database" , it will delete the item but we have archival is our end target. C,E makes a complete answer.

https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-importexport-ddb-pipelinejson-verifydata2.html

AWS Data Pipeline is a web service that you can use to automate the movement and transformation of data. With AWS Data Pipeline, you can define data-driven workflows, so that tasks can be dependent on the successful completion of previous tasks. You define the parameters of your data transformations and AWS Data Pipeline enforces the logic that you've set up.

please refer to the below URL https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html

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

QUESTION 212

A Solutions Architect is concerned that the current security group rules for a database tier are too permissive and may permit requests that should be restricted. Below are the current security group permissions for the database tier:

- **Protocol: TCP**
- **Port Range: 1433 (MS SQL)**
- **Source: ALL**

Currently, the only identified resource that needs to connect to the databases is the application tier consisting of an Auto Scaling group of EC2 instances.

What changes can be made to this security group that would offer the users LEAST privilege?

A. Change the source to -1 to remove source IP addresses previously unseen.
B. Change the source to the VPC CIDR block.
C. Change the source to the application instances IDs.
D. Change the source to the security group ID attached to the application instances.

Answer: D

"Security Group: Traffic can be restricted by any IP protocol, by service port, and source/destination IP address (individual IP or CIDR block)."

QUESTION 213

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

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-load-balancing.html

Host-based routing use host conditions to define rules that forward requests to different target groups based on the host name in the host header. This enables ALB to support multiple domains using a single load balancer. Path-based routing use path conditions to define rules that forward requests to different target groups based on the URL in the request. Each path condition has one path pattern. If the URL in a request matches the path pattern in a listener rule exactly, the request is routed using that rule. Only ALB supports Host-based & Path-based routing.

https://aws.amazon.com/blogs/aws/new-advanced-request-routing-for-aws-application-load-balancers/AWS Application Load Balancers have been around since the summer of 2016! They support content-based routing, work well for serverless & container-based applications, and are highly scalable. Many AWS customers are using the existing host and path-based routing to power their HTTP and HTTPS applications, while also taking advantage of other ALB features such as port forwarding (great for container-based applications), health checks, service discovery, redirects, fixed responses, and built-in authentication.

QUESTION 214
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 STANDARD_IA storage class after 15 days, and then to the GLACIER storage class after an additional 15 days.**
- **B. Create a lifecycle rule to transition the documents from the STANDARD storage class to the GLACIER storage class after 30 days.**
- **C. Create a lifecycle rule to transition documents from the STANDARD storage class to the STANDARD_IA storage class after 30 days and then to the GLACIER storage class after an additional 30 days.**
- **D. Create a lifecycle rule to transition the documents from the STANDARD storage class to the GLACIER storage class after 15 days.**

Answer: D

QUESTION 215

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. Configure lifecycle policies for the Amazon EC2 instances.**
- **D. Set up high-resolution alarms for the Auto Scaling group.**

Answer: B

memory utilization is one of the metrics not available by default in CloudWatch. Since AWS does not have access to the instance at the OS level, only metrics that can be monitored through the Hypervisor layer (such as CPU and Network Utilization) are recorded.

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

QUESTION 216
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

You can use cross-region replication to provide lower-latency data access in different geographic regions. I think is A because the data is update frequently and the new TTL=0 feature is excellent, is still pulling the data from the origin and not pushing. With A you push the data as soon as it changes.

QUESTION 217
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 CPU Utilization 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

Elastic Beanstalk automatically scales your application up and down based on your application's specific need using easily adjustable Auto Scaling settings. For example, you can use CPU utilization metrics to trigger Auto Scaling actions. With Elastic Beanstalk, your application can handle peaks in workload or traffic while minimizing your costs

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

QUESTION 218
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
https://www.purevpn.com/blog/whitelist-ip-addresses-on-aws/
https://aws.amazon.com/premiumsupport/knowledge-center/api-gateway-resource-policy-whitelist/

IP Whitelisting Explained

In simple terms, IP whitelisting is a feature that allows you to control and limit access based on a list of specified IP addresses. It's commonly used by administrators to prevent unauthorized parties from accessing corporate digital assets. While IP blacklisting also serves the same purpose, the way it does so is different – i.e. by identifying and blocking access to specified IP addresses.

QUESTION 219
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

QUESTION 220
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

QUESTION 221
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

QUESTION 222
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

QUESTION 223
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

QUESTION 224
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: AC

Going with A + C but my rationale on B, D and E being incorrect is as follows: B = Multiple containers aren't needed here as we are only putting the web application in there. Beanstalk to me = web applications, is having a DB in there even a choice? The MySQL DB can easily run in RDS without being in a container leaving a single container for the web application in Answer C. D & E- I'm taking this part of the question into consideration with these answers - "... that helps facilitate infrastructure management and deployment." The deployment part is sorted in this case but would Cloudformation and Lamba Custom Resources help with the management side of this as much as Beanstalk and ECS would? There's a small section in the Amazon documentation about Lamba-backed Custom Resources here: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-custom-resources-lambda.html

QUESTION 225
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.

QUESTION 226
What conditions could cause a Multi-AZ Amazon RDS failover to occur? (Choose two.)

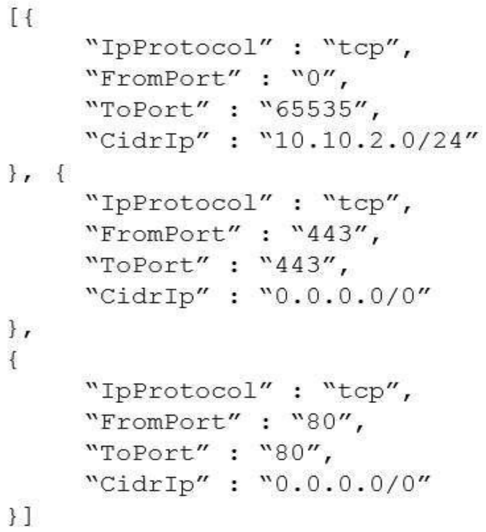
The RDS instance is stopped manually
A replica of the RDS instance is created in a different region
An Availability Zone becomes unavailable
Another master user is created
A failure of the primary database instance

QUESTION 227
A Solutions Architect is designing a new application that will be hosted on EC2 instances. This application has the following traffic requirements:

- **Accept HTTP(80)/HTTPS(443) traffic from the Internet.**
- **Accept FTP(21) traffic from the finance team servers at 10.10.2.0/24.**

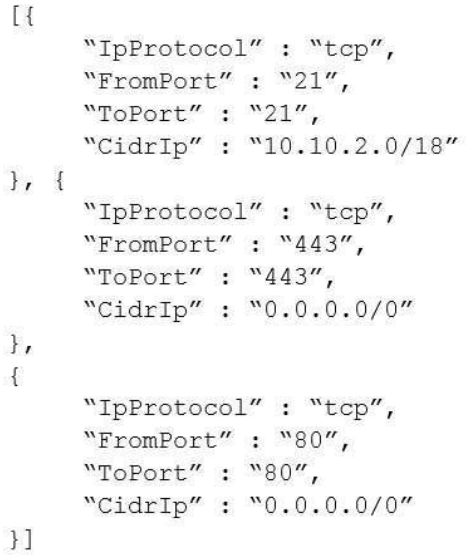
Which of the following AWS CloudFormation snippets correctly declares inbound security group rules that meet the requirements and prevent unauthorized access to additional services on the instance?

A



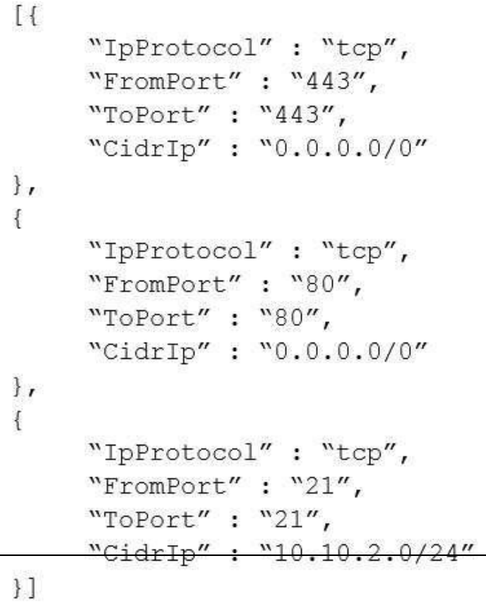
```
[{
      “IpProtocol” : “tcp”,
      “FromPort” : “0”,
      “ToPort” : “65535”,
      “CidrIp” : “10.10.2.0/24”
}, {
      “IpProtocol” : “tcp”,
      “FromPort” : “443”,
      “ToPort” : “443”,
      “CidrIp” : “0.0.0.0/0”
},
{
      “IpProtocol” : “tcp”,
      “FromPort” : “80”,
      “ToPort” : “80”,
      “CidrIp” : “0.0.0.0/0”
}]
```

B



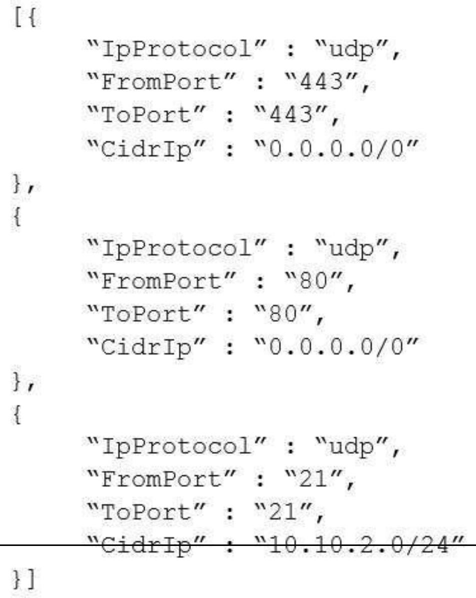
```
[{
      “IpProtocol” : “tcp”,
      “FromPort” : “21”,
      “ToPort” : “21”,
      “CidrIp” : “10.10.2.0/18”
}, {
      “IpProtocol” : “tcp”,
      “FromPort” : “443”,
      “ToPort” : “443”,
      “CidrIp” : “0.0.0.0/0”
},
{
      “IpProtocol” : “tcp”,
      “FromPort” : “80”,
      “ToPort” : “80”,
      “CidrIp” : “0.0.0.0/0”
}]
```

C.



```
[{
      “IpProtocol” : “tcp”,
      “FromPort” : “443”,
      “ToPort” : “443”,
      “CidrIp” : “0.0.0.0/0”
},
{
      “IpProtocol” : “tcp”,
      “FromPort” : “80”,
      “ToPort” : “80”,
      “CidrIp” : “0.0.0.0/0”
},
{
      “IpProtocol” : “tcp”,
      “FromPort” : “21”,
      “ToPort” : “21”,
      “CidrIp” : “10.10.2.0/24”
}]
```

D.



```
[{
      “IpProtocol” : “udp”,
      “FromPort” : “443”,
      “ToPort” : “443”,
      “CidrIp” : “0.0.0.0/0”
},
{
      “IpProtocol” : “udp”,
      “FromPort” : “80”,
      “ToPort” : “80”,
      “CidrIp” : “0.0.0.0/0”
},
{
      “IpProtocol” : “udp”,
      “FromPort” : “21”,
      “ToPort” : “21”,
      “CidrIp” : “10.10.2.0/24”
}]
```

QUESTION 228
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

QUESTION 229
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

QUESTION 230
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.

QUESTION 231
A company is moving to AWS. Management has identified a set of approved AWS services that meet all deployment requirements. The company would like to restrict access to all other unapproved services to which employees would have access.

Which solution meets these requirements with the LEAST amount of operational overhead?

A. Configure the AWS Trusted Advisor service utilization compliance report. Subscribe to Amazon SNS notifications from Trusted Advisor. Create a custom AWS Lambda function that can automatically remediate the use of unauthorized services.
B. Use AWS Config to evaluate the configuration settings of AWS resources. Subscribe to Amazon SNS notifications from AWS Config. Create a custom AWS Lambda function that can automatically remediate the use of unauthorized services.
C. Configure AWS Organizations. Create an organizational unit (OU) and place all AWS accounts into the OU. Apply a service control policy (SCP) to the OU that denies the use of certain services.
D. Create a custom AWS IAM policy. Deploy the policy to each account using AWS CloudFormation StackSets. Include deny statements in the policy to restrict the use of certain services. Attach the policies to all IAM users in each account.

Answer: C

QUESTION 232

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

QUESTION 233

A company is creating a web application that will run on an Amazon EC2 instance. The application on the instance needs access to an Amazon DynamoDB table for storage.

What should be done to meet these requirements?

A. **Create another AWS account root user with permissions to the DynamoDB table.**
B. **Create an IAM role and assign the role to the EC2 instance with permissions to the DynamoDB table.**
C. **Create an identity provider and assign the identity provider to the EC2 instance with permissions to the DynamoDB table.**
D. **Create identity federation with permissions to the DynamoDB table.**

Answer: B

QUESTION 234

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

QUESTION 235

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

QUESTION 236

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? (Choose 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: BC

QUESTION 237

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

QUESTION 238

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

it is temporary data and the most cost-efficient is instance storage. in a i3 instance is are nvme ssd disks, very fast storage:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html
i3.large has 475GB of SSD storage as instance store. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store-volumes

QUESTION 239

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

QUESTION 240
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

QUESTION 241
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

QUESTION 242
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

QUESTION 243
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

QUESTION 244
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
QUESTION 245
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
QUESTION 246
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
QUESTION 247
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.

QUESTION 248
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 Auto Scaling on the DynamoDB table.
C. Update the application to use strongly consistent reads.
D. Re-create the DynamoDB table with eventual consistency disabled.

QUESTION 249
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

QUESTION 250
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

QUESTION 251
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

QUESTION 252
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

QUESTION 253
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: C

QUESTION 254
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

QUESTION 255
How can a user track memory usage in an EC2 instance?

A. **Call Amazon CloudWatch to retrieve the memory usage metric data that exists for the EC2 instance.**
B. **Assign an IAM role to the EC2 instance with an IAM policy granting access to the desired metric.**
C. **Use an instance type that supports memory usage reporting to a metric by default.**
D. **Place an agent on the EC2 instance to push memory usage to an Amazon CloudWatch custom metric.**

Answer: D

QUESTION 256
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**

Asnwer: C

QUESTION 257
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

QUESTION 258
A Solutions 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? (Choose 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: CD

QUESTION 259
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

QUESTION 260
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
QUESTION 261
A company's Amazon RDS MySQL DB instance may be rebooted for maintenance and to apply patches. This database is critical and potential user disruption must be minimized.

What should the Solutions 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

QUESTION 262
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
QUESTION 263
A Solutions Architect is designing a new workload where an AWS Lambda function will access an Amazon DynamoDB table.

What is the MOST secure means of granting the Lambda function access to the DynamoDB table?

A. Create an identity and access management (IAM) role with the necessary permissions to access the DynamoDB table, and assign the role to the Lambda function.
B. Create a DynamoDB user name and password and give them to the Developer to use in the Lambda function.

C. **Create an identity and access management (IAM) user, and create access and secret keys for the user. Give the user the necessary permissions to access the DynamoDB table. Have the Developer use these keys to access the resources.**

D. **Create an identity and access management (IAM) role allowing access from AWS Lambda and assign the role to the DynamoDB table.**

Answer: A

QUESTION 264

A web application runs on Amazon EC2 instances behind an ELB Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones. Every night, the Auto Scaling group doubles in size. Traffic analysis shows that users in a particular region are requesting the same static content stored locally on the EC2 instances.

How can a Solutions Architect reduce the need to scale and improve application performance for the users?

A. **Re-deploy the application in a new VPC that is closer to the users making the requests.**

B. **Create an Amazon CloudFront distribution for the site and redirect user traffic to the distribution.**

C. **Store the contents on Amazon EFS instead of the EC2 root volume.**

D. **Implement Amazon Redshift to create a repository of the content closer to the users.**

Answer: B

QUESTION 265

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 ECS cluster security group to allow incoming access from the IP address of the ALB only.**

C. **Modify the security group used by the ECS 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

QUESTION 266

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

QUESTION 267

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? (Choose 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: CE
https://docs.aws.amazon.com/autoscaling/ec2/userguide/healthcheck.html

QUESTION 268
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
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/V2globaltables_HowItWorks.html
https://aws.amazon.com/dynamodb/global-tables/

QUESTION 269
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

QUESTION 270
A company needs to store data for 5 years. The company will need to have immediate and highly available access to the data at any point in time, but will not require frequent access.

What lifecycle action should be taken to meet the requirements while reducing costs?

A. Transition objects from Amazon S3 Standard to Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
B. Transition objects to expire after 5 years.
C. Transition objects from Amazon S3 Standard to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)
D. Transition objects from Amazon S3 Standard to the GLACIER storage class.

Answer: A
QUESTION 271
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

QUESTION 272
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? (Choose 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: AE
QUESTION 273
A company needs to use AWS resources to expand capacity for a website hosted in an on-premises data center. The AWS resources will include load balancers, Auto Scaling, and Amazon EC2 instances that will access an on-premises database. Network connectivity has been established, but no traffic is going to the AWS environment.

How should Amazon Route 53 be configured to distribute load to the AWS environment? (Choose 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: AB

QUESTION 274
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

QUESTION 275

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

egress-only is the option for IPV6

QUESTION 276

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: CD

QUESTION 277

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

QUESTION 278

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: AE

QUESTION 279

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

QUESTION 280

A Solutions 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 ?

QUESTION 281

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

QUESTION 282

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

QUESTION 283
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

QUESTION 284
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

QUESTION 285
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

QUESTION 286
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

QUESTION 287
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 URI.**
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

QUESTION 288
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 ?

QUESTION 289
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: BD ?

QUESTION 290
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

QUESTION 291
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

QUESTION 292
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: AB

QUESTION 293
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: AE

QUESTION 294

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 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: C

QUESTION 295

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

Is the only way for you to generate own keys on premise, use them to encrypt data and not have to store the keys on the cloud, still keep them on premise

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

QUESTION 296

A Solutions Architect is considering possible options for improving the security of the data on an Amazon EBS volume attached to an Amazon EC2 instance.

Which solution will improve the security of the data?

A. **Use AWS KMS to encrypt the EBS volume**
B. **Create an IAM policy that restricts read and write access to the volume**
C. **Migrate the sensitive data to an instance store volume**
D. **Use Amazon single sign-on to control login access to the EC2 instance**

Answer: A

QUESTION 297

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

QUESTION 298
A Solutions Architect is designing an application that requires having six Amazon EC2 instances running at all times. The application will be deployed in the sa-east-1 region, which has three Availability Zones: sa-east-1a, sa-east-1b, and sa-east-1c.

Which action will provide 100 percent fault tolerance and the LOWEST cost in the event that one Availability Zone in the region becomes unavailable?

A. Deploy six Amazon EC2 instances in sa-east-1a, six Amazon EC2 instances in sa-east-1b, and six Amazon EC2 instances in sa-east-1c
B. Deploy six Amazon EC2 instances in sa-east-1a, four Amazon EC2 instances in sa-east-1b, and two Amazon EC2 instances in sa-east-1c
C. Deploy three Amazon EC2 instances in sa-east-1a, three Amazon EC2 instances in sa-east-1b, and three Amazon EC2 instances in sa-east-1c
D. Deploy two Amazon EC2 instances in sa-east-1a, two Amazon EC2 instances in sa-east-1b, and two Amazon EC2 instances in sa-east-1c
Answer: C

QUESTION 299
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 subsecond 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

QUESTION 300
A Solutions Architect is designing an application in AWS. The Architect must not expose the application or database tier over the Internet for security reasons. The application must be low-cost and have a scalable front end. The databases and application tier must have only one-way Internet access to download software and patch updates.

Which solution helps to meet these requirements?

A. Use a NAT Gateway as the front end for the application tier and to enable the private resources to have Internet access.
B. Use an Amazon EC2-based proxy server as the front end for the application tier, and a NAT Gateway to allow Internet access for private resources.
C. Use an ELB Classic Load Balancer as the front end for the application tier, and an Amazon EC2 proxy server to allow Internet access for private resources.
D. Use an ELB Classic Load Balancer as the front end for the application tier, and a NAT Gateway to allow Internet access for private resources.

Answer: D

QUESTION 301
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

https://aws.amazon.com/datapipeline/

We use Security Groups for internal network design, ACLs are for external (Public).

QUESTION 302
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

QUESTION 303
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 ?

QUESTION 304

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

QUESTION 305

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

QUESTION 306

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

QUESTION 307

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

QUESTION 308

A company has thousands of files stored in an Amazon S3 bucket that has a well-defined access pattern. The files are accessed by an application multiple times a day for the 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

QUESTION 309

A company creates business-critical 3D images every night. The images are batch-processed every Friday and require an uninterrupted 48 hours to complete.

What is the MOST cost-effective Amazon EC2 pricing model for this scenario?

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

Answer: B

QUESTION 310

An application generates audit logs of operational activities. Compliance requirements mandate that the application retains 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

QUESTION 311

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

QUESTION 312
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

QUESTION 313
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? (Choose 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: BD

QUESTION 314
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 HTTP and HTTPS. Deny other traffic for inbound and outbound.
C. Allow inbound ports for HTTP and HTTPS 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

QUESTION 315
A company is launching a new static website on Amazon S3 and Amazon CloudFront. The company wants to ensure that all web requests go through only CloudFront.

How can a Solutions Architect meet this requirement?

A. Configure the S3 bucket policy to allow only CloudFront IP addresses to read objects.
B. Create IAM users in a group that has read access to the S3 bucket. Configure CloudFront to pass credentials to the S3 bucket.

C. **Create a CloudFront 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 CloudFront access to the instance by using security groups.**

Answer: C

QUESTION 316
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

QUESTION 317
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

QUESTION 318
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 securely on Amazon S3 and have the application generate an 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 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

QUESTION 319
An application calls a service run by a vendor. The vendor charges based on the number of calls. The finance department needs to know the number of calls that are made to the service to validate the billing statements.

How can a Solutions Architect design a system to durably store the number of calls without requiring changes to the application?

A. **Call the service through an internet gateway.**

B. Decouple the application from the service with an Amazon SQS queue.
C. Publish a custom Amazon CloudWatch metric that counts calls to the service.
D. Call the service through a VPC peering connection.

Answer: C

QUESTION 320

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

QUESTION 321

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 meet 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

QUESTION 322

An environment has an Auto Scaling group across two Availability Zones 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 EC2 instances and then continues to evaluate.
D. Auto Scaling terminates the instance with the closest next billing hour of all instances.

Answer: C

QUESTION 323

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 in 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

QUESTION 324

A Solutions Architect needs to convert potential single points of failure to a highly-available configuration. The current 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 Availability Zones and enable Multi-AZ RDS. Deploy a NAT gateway in one Availability Zone.

Answer: B

QUESTION 325

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

QUESTION 326

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

QUESTION 327

An application has components running in a public subnet and a private subnet. The components within the private subnet 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

QUESTION 328
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? (Choose two.)

A. Amazon ELB Application Load Balancer
B. Amazon ELB Classic Load Balancer
C. Amazon EC2 Container Service
D. Amazon DynamoDB
E. Amazon SQS

Answer: AC

QUESTION 329
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 it 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

QUESTION 330
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 seprate workers.
C. Increase the load balancer idle timeount to allow the long-running requests to complete.
D. Use Amazon ElastiCache for Redis to cache responses from the external service.

Answer :B

QUESTION 331
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 is unstructured and resides in Amazon S3.

What technology 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 (DAX).
D. Amazon ElastiCache for Redis with cluster mode enabled.

Answer: B

QUESTION 332
A Solutions 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 to process all the files uploaded each week. The application has built-in capabilities to process files in parallel, recover from the instance failures, 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

QUESTION 333
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? (Choose 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: AE

QUESTION 334
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 PostgreSQL database and point the dashboards at the Read Replica.
B. Move data from the RDS PostgreSQL database to Amazon Redshift nightly and point the dashboards at Amazon Redshift.
C. Monitor the database with Amazon CloudWatch and increase the instance size, 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 are pointed.

Answer: A

QUESTION 335
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

QUESTION 336
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

QUESTION 337
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

QUESTION 338
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

QUESTION 339
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

QUESTION 340

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

Aswer: C

QUESTION 341

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 Available Zone option and schedule periodic database snapshots.
D. Use Amazon DynamoDB.

Answer: B

QUESTION 342

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? (Choose 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 CloudWatch Events in the primary region that trigger the failover to the DR region

Answer: AC

QUESTION 343

A website keeps a record of user actions using a globally unique identifier (GIUD) retrieved from Amazon Aurora in place of the user name within the audit record. Security protocols state that the GUID content must not leave the company's Amazon VPC.

As the web traffic has increased, the number of web servers and Aurora read replicas has also increased to keep up with the user record reads 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 user's 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

QUESTION 344

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: D?

A is nto possible, see https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html "The NAT gateway sends the traffic to the internet gateway using the NAT gateway's Elastic IP address as the source IP address." Answer is D, because you need IGW already created when you created the NAT GW (so this rules out A)

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html o enable access to or from the internet for instances in a VPC subnet, you must do the following:Attach an internet gateway to your VPC.

There is a new question but I'm new to the site and not sure of the rules to contribute: A company is developing an application to deliver dynamic content to users around the globe. Thecontent should be customized according to a user's device and be delivered with very low latency. Which service should be used? A. Amazon API Gateway B. Amazon CloudFront C. Amazon S3 D. Lambda@Edge Answer: D The answer is D https://aws.amazon.com/lambda/edge/

https://aws.amazon.com/premiumsupport/knowledge-center/nat-gateway-vpc-private-subnet/ "Create a public VPC subnet to host the NAT gateway. The route table for the subnet should contain a route to the Internet through an Internet gateway." I think we can safely say that the IGW is already created beforehand in this scenario. Hence, it strengthens my choice of D.

QUESTION 345

A Solutions Architect is creating a multi-tiered architecture for an application that includes a public-facing web tier. Security requirements state that the Amazon EC2 instances 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. Implement an internet gateway on each VPC for external connectivity.

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 an internet gateway and use security groups to control communications between the layers.

Answer: D

QUESTION 346

A company is developing an application to deliver dynamic content to users around the globe. The content should be customized according to a user's device and be delivered with very low latency.

Which service should be used?

A. **Amazon API Gateway**
B. **Amazon CloudFront**
C. **Amazon S3**
D. **Lambda@Edge**

Answer: D

QUESTION 347

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

QUESTION 348

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

QUESTION 349

A company is designing a new application to collect data on user behavior for 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.