Practice Exam

AWS Certified Solutions Architect – Associate Exam

QUESTION 1

After an IT Steering Committee meeting, you have been put in charge of configuring a hybrid environment for the company's compute resources. You weigh the pros and cons of various technologies based on the requirements you are given. The main requirements to drive this selection are overall cost considerations and the ability to reuse existing internet connections. Which technology best meets these requirements?

- AWS Direct Connect
- VPC Peering
- AWS VPN
- AWS Direct Gateway

Answer | Flag for Review

QUESTION 2

Your company needs to deploy an application in the company AWS account. The application will reside on EC2 instances in an Auto Scaling Group fronted by an Application Load Balancer. The company has been using Elastic Beanstalk to deploy the application due to limited AWS experience within the organization. The application now needs upgrades and a small team of subcontractors have been hired to perform these upgrades. What can be used to provide the subcontractors with short-lived access tokens that act as temporary security credentials to the company AWS account?

- ○ IAM Roles
- ○ AWS SSO
- ○ AWS STS
- ○ IAM user accounts

QUESTION 3

A large financial institution is gradually moving their infrastructure and applications to AWS. The company has data needs that will utilize all of RDS, DynamoDB, Redshift, and ElastiCache. Which description best describes Amazon Redshift?

- ○ Key-value and document database that delivers single-digit millisecond performance at any scale.
- ○ Cloud-based relational database.
- ○ Can be used to significantly improve latency and throughput for many read-heavy application workloads.
- ○ Near real-time complex querying on massive data sets.

QUESTION 4

You have several EC2 instances in an auto scaling group fronted by a network load balancer. The instances will need access to S3 and DynamoDB. The auto scaling group was created from a launch template. What needs to be configured in the launch template to enable newly launched instances access to S3 and DynamoDB?

- An IAM Role attached to newly launched instances with permissions to S3 and DynamoDB.
- An IAM Group for EC2 with policies giving permission to S3 and DynamoDB.
- Access keys to be passed to newly launched EC2 instances.
- IAM policy attached to newly launched instances with permissions to S3 and DynamoDB.

Answer | Flag for Review

QUESTION 5

A software company is developing an online "learn a new language" application. The application will be designed to teach up to 20 different languages for native English and Spanish speakers. It is ideal that the application have fast response times and can deliver both text and voice to the end user. The application will also need to store user progress data. This application has 24,000 read units per second and 3,300 write units per second. Which type of storage would meet these requirements?

- S3
- EBS
- DynamoDB
- RDS

QUESTION 6

Your company has recently converted to a hybrid cloud environment and will slowly be migrating to a fully AWS cloud environment. The AWS side is in need of some steps to prepare for disaster recovery. A disaster recovery plan needs drawn up and disaster recovery drills need to be performed. The company wants to established Recovery Time and Recovery Point Objectives, with a major component being cost. You have determined and will recommend that the best DR configuration to meet cost and RTO/RPO objectives will be to have a minimal version of the application always running in another Region. Which AWS disaster recovery pattern will best meet these requirements?

- ○ Warm standby
- ○ Backup and restore
- ○ Pilot light
- ○ Multi-site

QUESTION 7

You are working in a large healthcare facility which uses EBS volumes on most of the EC2 instances. The CFO has approached you about some cost savings and it has been decided that some of the EC2 instances and EBS volumes would be deleted. What step can be taken to preserve the data on the EBS volumes and keep the data available on short notice?

- Move the data to Amazon S3.
- Archive the data to Glacier.
- Create and save a snapshot of the EBS volume in S3.
- Store the data in CloudFormation user data.

QUESTION 8

A database outage has been very costly to your organization. You have been tasked with configuring a more highly available architecture. The organization is willing to use any configuration necessary, and also use whatever database engine you recommend. Your initial recommendation is to use RDS Multi-AZ failover. Which of these RDS database engines does not use Amazon's failover technology?

- MySQL
- MariaDB
- SQL Server
- Oracle

QUESTION 9

A team of architects is designing a new AWS environment for a company which wants to migrate to the Cloud. The architects are considering the use of EC2 instances with instance store volumes. The architects realize that the data on the instance store volumes are ephemeral. Which action will not cause the data to be deleted on an instance store volume?

- ○ The underlying disk drive fails.
- ○ Reboot
- ○ Instance is stopped
- ○ Hardware disk failure.

QUESTION 10

A software company has created an application to capture service requests from users and also enhancement requests. The application is deployed on an Auto Scaling Group of EC2 instances fronted by an Application Load Balancer. The Auto Scaling Group has scaled to maximum capacity, but there are still requests being lost. The company has decided to use SQS with the Auto Scaling Group to ensure all messages are saved and processed. What is an appropriate metric for auto scaling with SQS?

- backlog per user
- backlog per instance
- backlog per hour
- cpu utilization

QUESTION 11

After an IT Steering Committee meeting you have been put in charge of configuring a hybrid environment for the company's compute resources. You weigh the pros and cons of various technologies based on the requirements you are given. Your primary requirement is the necessity for a private, dedicated connection, which bypasses the Internet and can provide throughput of 10 Gbps. Which option will you select?

- VPC Peering
- AWS Direct Gateway
- AWS VPN
- AWS Direct Connect

QUESTION 12

A software gaming company has produced an online racing game which uses CloudFront for fast delivery to worldwide users. The game also uses DynamoDB for storing in-game and historical user data. The DynamoDB table has a preconfigured read and write capacity. Users have been reporting slow down issues, and an analysis has revealed that the DynamoDB table has begun throttling during peak traffic times. Which step can you take to improve game performance?

- Add a load balancer in front of the web servers.
- Add an SQS Queue to queue requests which could be lost.
- Add ElastiCache to cache frequently accessed data in memory.
- Make sure DynamoDB Auto Scaling is turned on.

QUESTION 13

You have been tasked to review your company disaster recovery plan due to some new requirements. The driving factor is that the Recovery Time Objective has become very aggressive. Because of this, it has been decided to configure Multi-AZ deployments for the RDS MySQL databases. Unrelated to DR, it has been determined that some read traffic needs to be offloaded from the master database. What step can be taken to meet this requirement?

- Add read replicas to offload some read traffic.
- Redirect some of the read traffic to the standby database.
- Add DAX to the solution to alleviate excess read traffic.
- Convert to Aurora to allow the standby to serve read traffic.

QUESTION 14

You are about to configure two EC2 instances in your VPC. The instances will be in different subnets, but in the same Availability Zone. The first instance will house the main company website and will need to be able to communicate with the database that will be housed on the second instance. What steps can you take to make sure the instances will be able to communicate properly? Choose two.

(Choose 2)

- [ ] Configure a Virtual Private Gateway.
- [ ] Put the instances in the same placement group.
- [ ] Make sure all security groups allow communication between the app and database on the correct port using the proper protocol.
- [ ] Make sure each instance has an elastic IP address.
- [ ] Make sure the NACL allows communication between the two subnets.

QUESTION 15

You have configured an Auto Scaling Group of EC2 instances fronted by an Application Load Balancer. The back-end database is a MySQL RDS database. Your dev team has created a new AMI which has been hardened to meet company security standards, and this AMI needs to be deployed on all EC2 instances in the organization. What step or steps do you need to take to deploy this AMI?

- ○ Launch new instances with the AMI and add them to a new ALB Target Group.
- ○ Create a new launch configuration using this new AMI and then update your EC2 Auto Scaling Group with the new launch configuration.
- ○ Use a launch template instead of a launch configuration.
- ○ Do nothing. The Auto Scaling Group will recognize and use the new AMI.

QUESTION 16

An online media company has created an application which provides analytical data to its clients. The application is hosted on EC2 instances in an Auto Scaling Group. You have been brought on as a consultant and add an Application Load Balancer to front the Auto Scaling Group and distribute the load between the instances. The VPC which houses this architecture is running IPv4 and IPv6. The last thing you need to do to complete the configuration is point the domain name to the Application Load Balancer. Using Route 53, which record type at the zone apex will you use to point the DNS name of the Application Load Balancer? Choose two.

(Choose 2)

- [ ] Alias with a CNAME record set.
- [ ] Alias with an A type record set.
- [ ] Alias with an MX type record set.
- [ ] Alias with an AAAA type record set.

QUESTION 17

An application is hosted on an EC2 instance in a VPC. The instance is in a subnet in the VPC, and the instance has a public IP address. There is also an internet gateway and a security group with the proper ingress configured. But your testers are unable to access the instance from the Internet. What could be the problem?

- ○ Make sure the instance has a private IP address.
- ○ A √irtual private gateway needs to be configured.
- ○ A NAT gateway needs to be configured.
- ○ Add a route to the route table, from the subnet containing the instance, to the Internet Gateway.

QUESTION 18

Your company is storing stack traces for application errors in an S3 Bucket. The engineers using these stack traces review them when addressing application issues. It has been decided that the files only need to be kept for four weeks then they can be purged. How can you meet this requirement in S3?

- Configure the S3 Lifecycle rules to purge the files after a month.
- Create a bucket policy to purge the rules after one month.
- Add an S3 Lifecycle rule to archive these files to Glacier after one month.
- Write a cron job to purge the files after one month.

QUESTION 19

Your company is slowly migrating to the cloud and is currently in a hybrid environment. The server team has been provisioning servers to their exact specifications using Chef recipes. These recipes can be reused in AWS. Which AWS services are designed to work with existing Chef recipes?

- AWS Systems Manager
- CloudFormation
- Opsworks
- Elastic Beanstalk

QUESTION 20

After several issues with your application and unplanned downtime, your recommendation to migrate your application to AWS is approved. You have set up high availability on the front end with a load balancer and an Auto Scaling Group. What step can you take with your database to configure high-availability and ensure minimal downtime (under five minutes)?

- ○ Enable Multi-AZ failover on the database.
- ○ Create a read replica.
- ○ Create your database using CloudFormation and save the template for reuse.
- ○ Take frequent snapshots of your database.

QUESTION 21

Several S3 Buckets have been deleted and a few EC2 instances have been terminated. Which AWS service can you use to determine who took these actions?

- AWS Inspector
- Trusted Advisor
- AWS CloudTrail
- AWS CloudWatch

QUESTION 22

A car insurance company keeps specific details about accidents on file for a year, for quick retrieval, and then archives those files to long-term storage. A recent audit has approved the general steps they are taking, but pointed out many deficiencies in the technologies they are using. You have been hired as a consultant to come up with a solution. Your solution will recommend AWS storage options. What storage options could you recommend to meet the lifecycle requirements outlined, and provide high availability at a reasonable cost?

- Store the accident files in EBS volumes for a year, then migrate them to Glacier.
- Store the accident files in Glacier for maximum cost savings.
- Store the accident files in S3 for a year, then have the lifecycle policy move them to S3 IA
- Store the accident files in S3 for a year, then archive to Glacier.

QUESTION 23

A small startup company has begun using AWS for all of its IT infrastructure. The company has one AWS Solutions Architect and the demands for his time are overwhelming. The software team has been given permission to deploy their Python and PHP applications on their own. They would like to deploy these applications without having to worry about the underlying infrastructure. Which AWS service would they use for deployments?

- CodeDeploy
- CloudFront
- Elastic Beanstalk
- CloudFormation

QUESTION 24

You have just been hired by a large organization which uses many different AWS services in their environment. Some of the services which handle data include: RDS, Redshift, ElastiCache, DynamoDB, S3, and Glacier. You have been instructed to configure a web application using stateless web servers. Which services can you use to handle session state data? Choose two.

(Choose 2)

- [ ] DynamoDB
- [ ] Glacier
- [ ] Redshift
- [ ] Elasticache
- [ ] RDS

QUESTION 25

You have been given an assignment to configure Network ACLs in your VPC. Before configuring the NACLs, you need to understand how the NACLs are evaluated. How are NACL rules evaluated?

- ○ All NACL rules that you configure are evaluated before traffic is passed through.
- ○ NACL rules are evaluated by rule number from highest to lowest, and executed immediately when a matching rule is found.
- ○ NACL rules are evaluated by rule number from lowest to highest and executed immediately when a matching rule is found.
- ○ NACL rules are evaluated by rule number from highest to lowest, and all are evaluated before traffic is passed through.

QUESTION 26

You have been assigned to create an architecture which uses load balancers to direct traffic to an Auto Scaling Group of EC2 instances across multiple Availability Zones. The application to be deployed on these instances is a life insurance application which requires path-based and host-based routing. Which type of load balancer will you need to use?

- Any type of load balancer will meet these requirements.
- Network Load Balancer
- Classic Load Balancer
- Application Load Balancer

QUESTION 27

The CFO of your company approaches you and inquires about cutting costs in your AWS account. One area you are able to identify for cost cutting is in S3. There is data in S3 that is very rarely used and has only been retained for audit purposes. You decide to archive this data to a cheaper storage solution. Which AWS solution would meet this requirement?

- Use a lifecycle policy to archive the data to Glacier.
- Use a lifecycle policy to archive the data to Amazon SQS.
- Use a lifecycle policy to archive the data to Redshift.
- Write a cron job to archive the data to DynamoDB.

QUESTION 28

You have a typical architecture of an Application Load Balancer fronting an Auto Scaling Group of EC2 instances, backed by an RDS MySQL database. Your Application Load Balancer is performing health checks on the EC2 instances. What actions will be taken if an instance fails these health checks?

- ○ The instance is replaced by the ALB.
- ○ The ALB stops sending traffic to the instance.
- ○ The ALB notifies the Auto Scaling Group that the instance is down.
- ○ The instance is terminated by the ALB.

QUESTION 29

You have been tasked with designing a strategy for backing up EBS volumes attached to an instance-store-backed EC2 instance. You have been asked for an executive summary on your design, and the executive summary should include an answer to the question, "What can an EBS volume do when snapshotting the volume is in progress"?

- ○ The volume can only accommodate writes while a snapshot is in progress.
- ○ The volume can be used normally while the snapshot is in progress.
- ○ The volume can only accommodate reads while a snapshot is in progress.
- ○ The volume can not be used while a snapshot is in progress.

QUESTION 30

A travel company has deployed a website which serves travel updates to users all over the world. The traffic this database serves is very read heavy and can have some latency issues at certain times of the year. What can you do to alleviate these latency issues?

- Add read replicas
- Place CloudFront in front of the Database.
- Configure multi-Region RDS
- Configure RDS Multi-AZ

QUESTION 31

Your organization uses AWS CodeDeploy for deployments. Now you are starting a project on the AWS Lambda platform. For your deployments, you've been given a requirement of performing blue-green deployments. When you perform deployments, you want to split traffic, sending a small percentage of the traffic to the new version of your application. Which deployment configuration will allow this splitting of traffic?

- Canary
- Linear
- Weighted routing
- All at Once

QUESTION 32

Your company has decided to migrate a SQL Server database to a newly-created AWS account. Which service can be used to migrate the database?

- ○ Database Migration Service
- ○ DynamoDB
- ○ Elasticache
- ○ AWS RDS

QUESTION 33

You are working for a large financial institution and preparing for disaster recovery and upcoming DR drills. A key component in the DR plan will be the database instances and their data. An aggressive Recovery Time Objective (RTO) dictates that the database needs to be synchronously replicated. Which configuration can meet this requirement?

- AWS Lambda to trigger a CloudFormation template launch in another Region.
- RDS read replicas
- RDS Multi-AZ
- RDS Multi-Region

QUESTION 34

You have been assigned to create an architecture which uses load balancers to direct traffic to an Auto Scaling Group of EC2 instances across multiple Availability Zones. You were considering using an Application Load Balancer, but some of the requirements you have been given seem to point to a Classic Load Balancer. Which requirement would be better served by an Application Load Balancer?

- Support for EC2-Classic
- Path-based routing
- Support for TCP and SSL listeners
- Support for sticky sessions using application-generated cookies

QUESTION 35

You are designing an architecture for a financial company which provides a day trading application to customers. After viewing the traffic patterns for the existing application you notice that traffic is fairly steady throughout the day, with the exception of large spikes at the opening of the market in the morning and at closing around 3 pm. Your architecture will include an Auto Scaling Group of EC2 instances. How can you configure the Auto Scaling Group to ensure that system performance meets the increased demands at opening and closing of the market?

- Configure a Dynamic Scaling Policy to scale based on CPU Utilization.
- Use a load balancer to ensure that the load is distributed evenly during high-traffic periods.
- Configure your Auto Scaling Group to have a desired size which will be able to meet the demands of the high-traffic periods.
- Use a predictive scaling policy on the Auto Scaling Group to meet opening and closing spikes.

QUESTION 36

You have been evaluating the NACLS in your company. Most of the NACLs are configured the same: 100 All Traffic Allow 200 All Traffic Deny '' *All Traffic Deny What function does the* '' rule perform?

- It is there in case no other rules are defined.
- This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied.
- The * specifies that it is an example rule.
- Traffic will be denied from specified IP addresses.

QUESTION 37

Your company is using a hybrid configuration because there are some legacy applications which are not easily converted and migrated to AWS. And with this configuration comes a typical scenario where the legacy apps must maintain the same private IP address and MAC address. You are attempting to convert the application to the cloud and have configured an EC2 instance to house the application. What you are currently testing is removing the ENI from the legacy instance and attaching it to the EC2 instance. You want to attempt a cold attach. What does this mean?

- Attach ENI when it's stopped.
- Attach ENI to an instance when it's running.
- Attach ENI before the public IP address is assigned.
- Attach ENI when the instance is being launched.

QUESTION 38

You have recently migrated your small company to AWS and are looking for some general best practice guidance within the platform. Which AWS service can help you optimize your AWS environment by giving recommendations to reduce cost, increase security, and improve performance.

- AWS Inspector
- AWS Optimizations
- AWS Organizations
- AWS Trusted Advisor

QUESTION 39

You are working as a Solutions Architect for an online travel company. Your application is going to use an Auto Scaling Group of EC2 instances but you need to have some decoupling to store messages because of high volume. Which AWS service can be added to the solution that can meet this requirement?

- ○ RDS Read Replicas
- ○ Elasticache
- ○ AWS SQS
- ○ AWS Simple Workflow Service

QUESTION 40

Your company has recently converted to a hybrid cloud environment and will slowly be migrating to a fully AWS cloud environment. The AWS side is in need of some steps to prepare for disaster recovery. A disaster recovery plan needs drawn up and disaster recovery drills need to be performed for compliance reasons. The company wants to establish Recovery Time and Recovery Point Objectives. The RTO and RPO can be pretty relaxed. The main point is to have a plan in place, with as much cost savings as possible. Which AWS disaster recovery pattern will best meet these requirements?

- Backup and restore
- Warm Standby
- Multi Site
- Pilot Light

QUESTION 41

You work for an oil and gas company as a lead in data analytics. The company is using IoT devices to better understand their assets in the field (for example, pumps, generators, valve assemblies, and so on). Your task is to monitor the IoT devices in real-time to provide valuable insight that can help you maintain the reliability, availability, and performance of your IoT devices. What tool can you use to process streaming data in real time with standard SQL without having to learn new programming languages or processing frameworks?

- AWS Lambda
- AWS RedShift
- Kinesis Data Analytics
- AWS Kinesis Streams

QUESTION 42

A team member has been tasked to configure four EC2 instances for four separate applications. These are not high-traffic apps, so there is no need for an Auto Scaling Group. The instances are all in the same public subnet and each instance has an EIP address, and all of the instances have the same Security Group. But none of the instances can send or receive internet traffic. You verify that all the instances have a public IP address. You also verify that an internet gateway has been configured. What is the most likely issue?

- ○ There is no route in the route table to the internet gateway (or it has been deleted).
- ○ You are using the default nacl.
- ○ The route table is corrupt.
- ○ Each instance needs its own security group.

QUESTION 43

A new startup company decides to use AWS to host their web application. They configure a VPC as well as two subnets within the VPC. They also attach an internet gateway to the VPC. In the first subnet, they create an EC2 instance to host a web application. There is a network ACL and a security group, which both have the proper ingress and egress to and from the internet. There is a route in the route table to the internet gateway. The EC2 instances added to the subnet need to have a globally unique IP address to ensure internet access. Which is not a globally unique IP address?

- private IP address
- elastic IP address
- IPv6 address
- public IP address

QUESTION 44

You have been assigned to migrate an application and the servers it runs on to the company AWS cloud environment. You have created a checklist of steps necessary to perform this migration. A subsection in the checklist is security considerations. One of the things that you need to consider is the shared responsibility module. Which option does the customer handle under the shared responsibility model?

- Network infrastructure
- Hardware infrastructure
- Identity and Access Management
- Availability Zones

QUESTION 45

A software company has produced several stateless applications. The software team now needs servers to act as test servers for these applications. These servers are not mission-critical, so occasional downtime is acceptable. What type of EC2 servers can be used to meet these requirements at the lowest cost?

- Dedicated Hosts
- Spot
- Reserved
- On-Demand

QUESTION 46

A consultant hired by a small company to configure an AWS environment. The consultant begins working with the VPC and launching EC2 instances within the VPC. The initial instances will be placed in a public subnet. The consultant begins to create security groups. What is true of security groups?

- ○ You can specify allow rules but not deny rules.
- ○ You can specify deny rules, but not allow rules.
- ○ By default, a security group includes an inbound rule that allows all inbound traffic.
- ○ You can't specify separate rules for inbound and outbound traffic.

QUESTION 47

You are put in charge of your company's Disaster Recovery planning. As part of this plan, you intend to create all of the company infrastructure with CloudFormation templates. The templates can then be saved in another region and used to launch a new environment in case of disaster. What determines the costs associated with CloudFormation templates?

- It depends whether the resources in the template are in the free tier.
- The distance of the region from the home region.
- There is no cost for templates, but when deployed, the resources created will accumulate charges.
- There is a cost per template and discounts for over 100 templates.

QUESTION 48

A small software team is creating an application which will give subscribers real-time weather updates. The application will run on EC2 and will make several requests to AWS services such as S3 and DynamoDB. What is the best way to grant permissions to these other AWS services?

- Create an IAM policy that you attach to the EC2 instance to give temporary security credentials to applications running on the instance.
- Create an IAM user, grant the user permissions, and pass the user credentials to the application.
- Create an IAM role that you attach to the EC2 instance to give temporary security credentials to applications running on the instance.
- Embed the appropriate credentials to access AWS services in the application.

QUESTION 49

You have been tasked with migrating an application and the servers it runs on to the company AWS cloud environment. You have created a checklist of steps necessary to perform this migration. A subsection in the checklist is security considerations. One of the things that you need to consider is the shared responsibility module. Which option does AWS handle under the shared responsibility model?

- Client-side data encryption
- User Authentication
- Firewall Configuration
- Physical Hardware Infrastructure

QUESTION 50

An insurance company is creating an application which will perform analytics in near real-time on huge datasets in the terabyte range and potentially even petabyte. The company is evaluating an AWS data storage option. Which AWS service will allow storage of petabyte scale data and also allow fast querying of this data?

- DynamoDb
- Redshift
- ElastiCache
- RDS

QUESTION 51

A company has a great deal of data in S3 buckets for which they want to create a database. Creating the RDS database, normalizing the data, and migrating to the RDS database will take time and is the long-term plan. But there's an immediate need to query this data to retrieve information necessary for an audit. Which AWS service will enable querying data in S3 using standard SQL commands?

- Amazon SQL Connector
- Amazon Athena
- There is no such service, but there are third-party tools.
- DynamoDB

QUESTION 52

A consultant is hired by a small company to configure an AWS environment. The consultant begins working with the VPC and launching EC2 instances within the VPC. The initial instances will be placed in a public subnet. The consultant begins to create security groups. The consultant has launched several instances, created security groups, and has associated security groups with instances. The consultant wants to change the security groups for an instance. Which statement is true?

- ○ You can't change security groups. Create a new instance and attach the desired security groups.
- ○ You can change the security groups for an instance when the instance is in the pending or stopped state.
- ○ You can't change the security groups for an instance when the instance is in the running or stopped state.
- ○ You can change the security groups for an instance when the instance is in the running or stopped state.

QUESTION 53

Your company has asked you to look into some latency issues with the company web app. The application is backed by an AWS RDS database. Your analysis has determined that the requests made of the application are very read heavy, and this is where improvements can be made. Which service can you use to store frequently accessed data in-memory?

- ElastiCache
- EBS
- DynamoDB
- DAX

QUESTION 54

A consultant is hired by a small company to configure an AWS environment. The consultant begins working with the VPC and launching EC2 instances within the VPC. The initial instances will be placed in a public subnet. The consultant begins to create security groups. What is true of the default security group?

- ○ You can't delete this group, nor can you change the group's rules.
- ○ You can delete this group or you can change the group's rules.
- ○ You can't delete this group, however, you can change the group's rules.
- ○ You can delete this group, however, you can't change the group's rules.

QUESTION 55

A data company has implemented a subscription service for storing video files. There are two levels of subscription: personal and professional use. The personal users can upload a total of 5 GB of data, and professional users can upload as much as 5 TB of data. The application can upload files of size up to 1 TB to an S3 Bucket. What is the best way to upload files of this size?

- AWS SnowMobile
- Multipart upload
- AWS Snowball
- Single-part Upload

QUESTION 56

A financial institution has an application that produces huge amounts of actuary data, which is ultimately expected to be in the terabyte range. There is a need to run complex analytic queries against terabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution. Which storage service will best meet this requirement?

- Elasticache
- Redshift
- DynamoDB
- RDS

QUESTION 58

You have configured an Auto Scaling Group of EC2 instances. You have begun testing the scaling of the Auto Scaling Group using a stress tool to force the CPU utilization metric being used to force scale out actions. The stress tool is also being manipulated by removing stress to force a scale in. But you notice that these actions are only taking place in five-minute intervals. What is happening?

- ○ A load balancer is managing the load and limiting the effectiveness of stressing the servers.
- ○ Auto Scaling Groups can only scale in intervals of five minutes or greater.
- ○ The stress tool is configured to run for five minutes.
- ○ The Auto Scaling Group is following the default cooldown procedure.

QUESTION 58

You have configured an Auto Scaling Group of EC2 instances. You have begun testing the scaling of the Auto Scaling Group using a stress tool to force the CPU utilization metric being used to force scale out actions. The stress tool is also being manipulated by removing stress to force a scale in. But you notice that these actions are only taking place in five-minute intervals. What is happening?

- ○ A load balancer is managing the load and limiting the effectiveness of stressing the servers.
- ○ Auto Scaling Groups can only scale in intervals of five minutes or greater.
- ○ The stress tool is configured to run for five minutes.
- ○ The Auto Scaling Group is following the default cooldown procedure.

QUESTION 59

After an IT Steering Committee meeting, you have been put in charge of configuring a hybrid environment for the company's compute resources. You weigh the pros and cons of various technologies, such as VPN and Direct Connect, and based on the requirements you have decided to configure a VPN connection. What features and advantages can a VPN connection provide?

- It provides a connection between an on-premises network and a VPC, using a secure and private connection with IPsec and TLS.
- It provides a private, dedicated network connection between an on-premises network and the VPC.
- It provides a network connection between two VPCs that can route traffic using IPv4 or IPv6.
- It provides a cost-effective, private network connection that bypasses the internet.

QUESTION 60

A database outage has been very costly to your organization. You have been tasked with configuring a more highly-available architecture. The main requirement is that the chosen architecture needs to meet an aggressive RTO in case of disaster. You have decided to use an RDS Multi-AZ deployment. How is the replication handled for RDS Multi-AZ?

- Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Region.
- Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone.
- Amazon RDS automatically provisions and maintains an asynchronous standby replica in a different Availability Zone.
- You can configure a standby replica in a different Availability Zone and send traffic synchronously or asynchronously depending on your cost considerations.

QUESTION 61

A small company has nearly 200 users who already have AWS accounts in the company AWS environment. A new S3 bucket has been created which will allow roughly a third of all users access to sensitive information in the bucket. What is the most time efficient way to get these users access to the bucket?

- Create a new bucket policy granting the appropriate permissions and attach it to the bucket.
- Create a new policy which will grant permissions to the bucket. Create a group and attach the policy to that group. Add the users to this group.
- Create a new role which will grant permissions to the bucket. Create a group and attach the role to that group. Add the users to this group.
- Create a new policy which will grant permissions to the bucket. Create a role and attach the policy to that role. Add the users to this role.

QUESTION 62

An international travel company has an application which provides travel information and alerts to users all over the world. The application is hosted on groups of EC2 instances in Auto Scaling Groups in multiple AWS Regions. There are also load balancers routing traffic to these instances. In two countries, Ireland and Australia, there are compliance rules in place that dictate users connect to the application in eu-west-1 and ap-southeast-1. Which service can you use to meet this requirement?

- Configure CloudFront and the users will be routed to the nearest edge location.
- Use Route 53 weighted routing.
- Use Route 53 geolocation routing.
- Configure the load balancers to route users to the proper region.

QUESTION 63

A consultant hired by a small company to configure an AWS environment. The consultant begins working with the VPC and launching EC2 instances within the VPC. The initial instances will be placed in a public subnet. The consultant begins to create security groups. What is true of security groups?

- Security groups act at the instance level, not the subnet level.
- Security groups act at the subnet level, not the instance level.
- Security groups act at the VPC level, not the instance level.
- Security groups are stateless.

QUESTION 64

A new startup company decides to use AWS to host their web application. They configure a VPC as well as two subnets within the VPC. They also attach an internet gateway to the VPC. In the first subnet, they create the EC2 instance which will host their web application. They finish the configuration by making the application accessible from the Internet. The second subnet has an instance hosting a smaller, secondary application. But this application is not currently accessible from the Internet. What could be potential problems?

(Choose 2)

- [ ] The second subnet does not have a route in the route table to the internet gateway.
- [ ] The second subnet does not have a route in the route table to the virtual private gateway.
- [ ] The EC2 instance does not have a public IP address.
- [ ] The EC2 instance is not attached to an internet gateway.
- [ ] The second subnet does not have a public IP address.

QUESTION 65

The AWS team in a large company is spending a lot of time monitoring EC2 instances and maintenance when the instances report health check failures. How can you most efficiently automate this monitoring and repair?

- Create a Lambda function which can be triggered by a failed instance health check. Have the Lambda function destroy the instance and spin up a new instance.
- Create a Lambda function which can be triggered by a failed instance health check. Have the Lambda function deploy a CloudFormation template which can perform the creation of a new instance.
- Create a cron job which monitors the instances periodically and starts a new instance if a health check has failed.
- Create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically reboots the instance if a health check fails.

Answers

QUESTION 1

After an IT Steering Committee meeting, you have been put in charge of configuring a hybrid environment for the company's compute resources. You weigh the pros and cons of various technologies based on the requirements you are given. The main requirements to drive this selection are overall cost considerations and the ability to reuse existing internet connections. Which technology best meets these requirements?

- ✗ AWS Direct Connect Selected
- ✗ VPC Peering
- ✓ AWS VPN
- ✗ AWS Direct Gateway

EXPLANATION

Incorrect: Direct Connect does not use the internet.

AWS Managed VPN lets you reuse existing VPN equipment and processes, and reuse existing internet connections.

It is an AWS-managed high availability VPN service.

It supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies.

QUESTION 2

Your company needs to deploy an application in the company AWS account. The application will reside on EC2 instances in an Auto Scaling Group fronted by an Application Load Balancer. The company has been using Elastic Beanstalk to deploy the application due to limited AWS experience within the organization. The application now needs upgrades and a small team of subcontractors have been hired to perform these upgrades. What can be used to provide the subcontractors with short-lived access tokens that act as temporary security credentials to the company AWS account?

- ✗ IAM Roles
- ✗ AWS SSO
- ✓ AWS STS Selected
- ✗ IAM user accounts

EXPLANATION

Correct. AWS Security Token Service (AWS STS) is the service that you can use to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use. You can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use, with the following differences: Temporary security credentials are short-term, as the name implies. They can be configured to last for anywhere from a few minutes to several hours. After the credentials expire, AWS no longer recognizes them or allows any kind of access from API requests made with them. Temporary security credentials are not stored with the user but are generated dynamically and provided to the user when requested. When (or even before) the temporary security credentials expire, the user can request new credentials, as long as the user requesting them still has permissions to do so. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

QUESTION 3

A large financial institution is gradually moving their infrastructure and applications to AWS. The company has data needs that will utilize all of RDS, DynamoDB, Redshift, and ElastiCache. Which description best describes Amazon Redshift?

- ✗ Key-value and document database that delivers single-digit millisecond performance at any scale.
- ✗ Cloud-based relational database.
- ✗ Can be used to significantly improve latency and throughput for many read-heavy application workloads.
- ✓ Near real-time complex querying on massive data sets. Selected

EXPLANATION

Amazon Redshift is a fast, fully-managed cloud data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It allows you to run complex analytic queries against terabytes to petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution. Most results come back in seconds. With Redshift, you can start small for just $0.25 per hour with no commitments and scale out to petabytes of data for $1,000 per terabyte per year, less than a tenth the cost of traditional on-premises solutions. Amazon Redshift also includes Amazon Redshift Spectrum, allowing you to run SQL queries directly against exabytes of unstructured data in Amazon S3 data lakes. No loading or transformation is required, and you can use open data formats, including Avro, CSV, Grok, Amazon Ion, JSON, ORC, Parquet, RCFile, RegexSerDe, Sequence, Text, and TSV. Redshift Spectrum automatically scales query compute capacity based on the data retrieved, so queries against Amazon S3 run fast, regardless of data set size. https://aws.amazon.com/redshift/faqs/

QUESTION 4

You have several EC2 instances in an auto scaling group fronted by a network load balancer. The instances will need access to S3 and DynamoDB. The auto scaling group was created from a launch template. What needs to be configured in the launch template to enable newly launched instances access to S3 and DynamoDB?

- ✓ An IAM Role attached to newly launched instances with permissions to S3 and DynamoDB.
- ✗ An IAM Group for EC2 with policies giving permission to S3 and DynamoDB. Selected
- ✗ Access keys to be passed to newly launched EC2 instances.
- ✗ IAM policy attached to newly launched instances with permissions to S3 and DynamoDB.

EXPLANATION

Incorrect. Groups can be used to grant a group of users specific permissions based on the policies attached to the group, but groups are not used with EC2 instances.

Correct. IAM roles are designed 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.

QUESTION 5

A software company is developing an online "learn a new language" application. The application will be designed to teach up to 20 different languages for native English and Spanish speakers. It is ideal that the application have fast response times and can deliver both text and voice to the end user. The application will also need to store user progress data. This application has 24,000 read units per second and 3,300 write units per second. Which type of storage would meet these requirements?

- ✗ S3 Selected
- ✗ EBS
- ✓ DynamoDB
- ✗ RDS

EXPLANATION

Incorrect. This type of requirement, specifically the fast response times, is better suited for DynamoDB.

Correct. Duolingo uses Amazon DynamoDB to store 31 billion items in support of an online learning site that delivers lessons for 80 languages. The U.S. startup reaches more than 18 million monthly users around the world who perform more than six billion exercises using the free Duolingo lessons. The company relies heavily on Amazon DynamoDB not just for its highly scalable database, but also for high performance that reaches 24,000 read units per second and 3,300 write units per second. In addition, Duolingo uses a range of other AWS services such as Amazon EC2, based on the latest Intel Xeon Processor Family, for compute Amazon ElastiCache to increase performance; Amazon S3 for storing image-related data; and Amazon Relational Database Service (Amazon RDS) for permanent data storage. Moving forward, Duolingo plans on leveraging AWS Elastic Beanstalk and AWS Lambda for its microservices architecture, as well as Amazon Redshift for its data analytics. https://aws.amazon.com/solutions/case-studies/duolingo-case-study-dynamodb/

QUESTION 6

Your company has recently converted to a hybrid cloud environment and will slowly be migrating to a fully AWS cloud environment. The AWS side is in need of some steps to prepare for disaster recovery. A disaster recovery plan needs drawn up and disaster recovery drills need to be performed. The company wants to established Recovery Time and Recovery Point Objectives, with a major component being cost. You have determined and will recommend that the best DR configuration to meet cost and RTO/RPO objectives will be to have a minimal version of the application always running in another Region. Which AWS disaster recovery pattern will best meet these requirements?

- ✗ Warm standby
- ✗ Backup and restore
- ✓ Pilot light Selected
- ✗ Multi-site

EXPLANATION

Correct. 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.

QUESTION 7

You are working in a large healthcare facility which uses EBS volumes on most of the EC2 instances. The CFO has approached you about some cost savings and it has been decided that some of the EC2 instances and EBS volumes would be deleted. What step can be taken to preserve the data on the EBS volumes and keep the data available on short notice?

- ✗ Move the data to Amazon S3. Selected
- ✗ Archive the data to Glacier.
- ✓ Create and save a snapshot of the EBS volume in S3.
- ✗ Store the data in CloudFormation user data.

EXPLANATION

Incorrect: Although snapshots are ultimately stored in S3, there is a more specific answer. This answer suggests manually moving the snapshot to S3.

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information that is needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume.

QUESTION 8

A database outage has been very costly to your organization. You have been tasked with configuring a more highly available architecture. The organization is willing to use any configuration necessary, and also use whatever database engine you recommend. Your initial recommendation is to use RDS Multi-AZ failover. Which of these RDS database engines does not use Amazon's failover technology?

- ✗ MySQL
- ✗ MariaDB
- ✓ SQL Server Selected
- ✗ Oracle

EXPLANATION

Correct: Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. Multi-AZ deployments for MariaDB, MySQL, Oracle, and PostgreSQL instances use Amazon's failover technology. SQL Server instances use SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs).

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary database instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a database instance with high availability can enhance availability during planned system maintenance, and helps protect your databases against instance failure and Availability Zone disruption.

QUESTION 9

A team of architects is designing a new AWS environment for a company which wants to migrate to the Cloud. The architects are considering the use of EC2 instances with instance store volumes. The architects realize that the data on the instance store volumes are ephemeral. Which action will not cause the data to be deleted on an instance store volume?

- ✗ The underlying disk drive fails.
- ✓ Reboot
- ✗ Instance is stopped Selected
- ✗ Hardware disk failure.

EXPLANATION

Incorrect. The data in an instance store persists only during the lifetime of its associated instance.

Correct. Some Amazon Elastic Compute Cloud (Amazon EC2) instance types come with a form of directly attached, block-device storage known as the instance store. The instance store is ideal for temporary storage, because the data stored in instance store volumes is not persistent through instance stops, terminations, or hardware failures.

QUESTION 10

A software company has created an application to capture service requests from users and also enhancement requests. The application is deployed on an Auto Scaling Group of EC2 instances fronted by an Application Load Balancer. The Auto Scaling Group has scaled to maximum capacity, but there are still requests being lost. The company has decided to use SQS with the Auto Scaling Group to ensure all messages are saved and processed. What is an appropriate metric for auto scaling with SQS?

- ✗ backlog per user
- ✓ backlog per instance
- ✗ backlog per hour
- ✗ cpu utilization Selected

EXPLANATION

Incorrect. As the name implies, this metric will report on the percentage of utilization on the CPU.

The issue with using a CloudWatch Amazon SQS metric like ApproximateNumberOfMessagesVisible for target tracking is that the number of messages in the queue might not change proportionally to the size of the Auto Scaling Group that processes messages from the queue. That's because the number of messages in your SQS queue does not solely define the number of instances needed. The number of instances in your Auto Scaling Group can be driven by multiple factors, including how long it takes to process a message and the acceptable amount of latency (queue delay). The solution is to use a backlog per instance metric with the target value being the acceptable backlog per instance to maintain. You can calculate these numbers as follows: Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling Group is the number of instances in the InService state, to get the backlog per instance.

QUESTION 11

After an IT Steering Committee meeting you have been put in charge of configuring a hybrid environment for the company's compute resources. You weigh the pros and cons of various technologies based on the requirements you are given. Your primary requirement is the necessity for a private, dedicated connection, which bypasses the Internet and can provide throughput of 10 Gbps. Which option will you select?

- ✗ VPC Peering
- ✗ AWS Direct Gateway Selected
- ✗ AWS VPN
- ✓ AWS Direct Connect

EXPLANATION

Incorrect. This is not a real service.

Correct. AWS Direct Connect can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections. It uses industry-standard 802.1q VLANs to connect to Amazon VPC using private IP addresses. You can choose from an ecosystem of WAN service providers for integrating your AWS Direct Connect endpoint in an AWS Direct Connect location with your remote networks. AWS Direct Connect lets you establish 1 Gbps or 10 Gbps dedicated network connections (or multiple connections) between AWS networks and one of the AWS Direct Connect locations. You can also work with your provider to create sub-1G connection or use link aggregation group (LAG) to aggregate multiple 1 gigabit or 10 gigabit connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection. A Direct Connect gateway is a globally available resource to enable connections to multiple Amazon VPCs across different regions or AWS accounts. https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect.html

QUESTION 12

A software gaming company has produced an online racing game which uses CloudFront for fast delivery to worldwide users. The game also uses DynamoDB for storing in-game and historical user data. The DynamoDB table has a preconfigured read and write capacity. Users have been reporting slow down issues, and an analysis has revealed that the DynamoDB table has begun throttling during peak traffic times. Which step can you take to improve game performance?

- ✗ Add a load balancer in front of the web servers.
- ✗ Add an SQS Queue to queue requests which could be lost.
- ✗ Add ElastiCache to cache frequently accessed data in memory. Selected
- ✓ Make sure DynamoDB Auto Scaling is turned on.

EXPLANATION

Incorrect. ElastiCache is not intended for use with DynamoDB.

Correct: 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. Note that if you use the AWS Management Console to create a table or a global secondary index, DynamoDB auto scaling is enabled by default. You can modify your auto scaling settings at any time.

QUESTION 13

You have been tasked to review your company disaster recovery plan due to some new requirements. The driving factor is that the Recovery Time Objective has become very aggressive. Because of this, it has been decided to configure Multi-AZ deployments for the RDS MySQL databases. Unrelated to DR, it has been determined that some read traffic needs to be offloaded from the master database. What step can be taken to meet this requirement?

- ✓ Add read replicas to offload some read traffic. Selected
- ✗ Redirect some of the read traffic to the standby database.
- ✗ Add DAX to the solution to alleviate excess read traffic.
- ✗ Convert to Aurora to allow the standby to serve read traffic.

EXPLANATION

Amazon RDS Read Replicas for MySQL and MariaDB now support Multi-AZ deployments. Combining Read Replicas with Multi-AZ enables you to build a resilient disaster recovery strategy and simplify your database engine upgrade process. Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed. https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/#:~:text=Amazon%20RDS%20Read%20Replicas%20Now%20Support%20Multi%2DAZ%20Deployments,-Posted%20On%3A%20Jan&text=Amazon%20RDS%20Read%20Replicas%20enable,copied%20to%20your%20Read%20Replicas.

QUESTION 14

You are about to configure two EC2 instances in your VPC. The instances will be in different subnets, but in the same Availability Zone. The first instance will house the main company website and will need to be able to communicate with the database that will be housed on the second instance. What steps can you take to make sure the instances will be able to communicate properly? Choose two.

- ✗ Configure a Virtual Private Gateway. Selected
- ✗ Put the instances in the same placement group.
- ✓ Make sure all security groups allow communication between the app and database on the correct port using the proper protocol.
- ✗ Make sure each instance has an elastic IP address.
- ✓ Make sure the NACL allows communication between the two subnets. Selected

EXPLANATION

Incorrect. VPWs are suited for setting up VPN connections. The instances are in the same VPC and Availability Zones. A VPW is not needed.

Correct: The proper ingress on both the security groups and NACL need to be configured to allow communication between these instances.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html

Correct: The proper ingress on both the Security Groups and NACL need to be configured to allow communication between these instances.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html

QUESTION 15

You have configured an Auto Scaling Group of EC2 instances fronted by an Application Load Balancer. The back-end database is a MySQL RDS database. Your dev team has created a new AMI which has been hardened to meet company security standards, and this AMI needs to be deployed on all EC2 instances in the organization. What step or steps do you need to take to deploy this AMI?

- ✗ Launch new instances with the AMI and add them to a new ALB Target Group.
- ✓ Create a new launch configuration using this new AMI and then update your EC2 Auto Scaling Group with the new launch configuration.
- ✗ Use a launch template instead of a launch configuration. Selected
- ✗ Do nothing. The Auto Scaling Group will recognize and use the new AMI.

EXPLANATION

Incorrect. This answer does not provide enough detail.

A launch configuration is an instance configuration template that an Auto Scaling Group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances. Include the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping. If you've launched an EC2 instance before, you specified the same information in order to launch the instance. You can specify your launch configuration with multiple Auto Scaling Groups. However, you can only specify one launch configuration for an Auto Scaling Group at a time, and you can't modify a launch configuration after you've created it. To change the launch configuration for an Auto Scaling Group, you must create a launch configuration and then update your Auto Scaling Group with it.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html

QUESTION 16

An online media company has created an application which provides analytical data to its clients. The application is hosted on EC2 instances in an Auto Scaling Group. You have been brought on as a consultant and add an Application Load Balancer to front the Auto Scaling Group and distribute the load between the instances. The VPC which houses this architecture is running IPv4 and IPv6. The last thing you need to do to complete the configuration is point the domain name to the Application Load Balancer. Using Route 53, which record type at the zone apex will you use to point the DNS name of the Application Load Balancer? Choose two.

- ✗ Alias with a CNAME record set. Selected
- ✓ Alias with an A type record set.
- ✗ Alias with an MX type record set. Selected
- ✓ Alias with an AAAA type record set.

EXPLANATION

Incorrect. Alias with a type "CNAME" record set is incorrect because you can't create a CNAME record at the zone apex.

Alias with a type of "MX" record set is incorrect because an MX record is primarily used for mail servers.

Alias with a type "AAAA" record set and Alias with a type "A" record set are correct. To route domain traffic to an ELB load balancer, use Amazon Route 53 to create an alias record that points to your load balancer. An alias record is a Route 53 extension to DNS.

Alias with a type "AAAA" record set and Alias with a type "A" record set are correct. To route domain traffic to an ELB, use Amazon Route 53 to create an alias record that points to your load balancer.

QUESTION 17

An application is hosted on an EC2 instance in a VPC. The instance is in a subnet in the VPC, and the instance has a public IP address. There is also an internet gateway and a security group with the proper ingress configured. But your testers are unable to access the instance from the Internet. What could be the problem?

- ✗ Make sure the instance has a private IP address.
- ✗ A √irtual private gateway needs to be configured.
- ✗ A NAT gateway needs to be configured.
- ✓ Add a route to the route table, from the subnet containing the instance, to the Internet Gateway. Selected

EXPLANATION

Correct. The question doesn't state if the subnet containing the instance is public or private. An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. To enable access to or from the internet for instances in a subnet in a VPC, you must do the following:

- Attach an internet gateway to your VPC.
- Add a route to your subnet's route table that directs internet-bound traffic to the internet gateway. If a subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet. If a subnet is associated with a route table that does not have a route to an internet gateway, it's known as a private subnet.
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control lists and security group rules allow the relevant traffic to flow to and from your instance.
- In your subnet route table, you can specify a route for the internet gateway to all destinations not explicitly known to the route table (0.0.0.0/0 for IPv4 or ::/0 for IPv6). Alternatively, you can scope the route to a narrower range of IP addresses. For example, the public IPv4 addresses of your company's public endpoints outside of AWS, or the elastic IP addresses of other Amazon EC2 instances outside your VPC. To enable communication over the Internet for IPv4, your instance must have a public IPv4 address or an Elastic IP address that's associated with a private IPv4 address on your instance. Your instance is only aware of the private (internal) IP address space defined within the VPC and subnet. The internet gateway logically provides the one-to-one NAT on behalf of your instance so that when traffic leaves your VPC subnet and goes to the Internet, the reply address field is set to the public IPv4 address or elastic IP address of your instance and not its private IP address. Conversely, traffic that's destined for the public IPv4 address or elastic IP address of your instance has its destination address translated into the instance's private IPv4 address before the traffic is delivered to the VPC. To enable communication over the Internet for IPv6, your VPC and subnet must have an associated IPv6 CIDR block, and your instance must be assigned an IPv6 address from the range of the subnet. IPv6 addresses are globally unique, and therefore public by default.
  https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

QUESTION 18

Your company is storing stack traces for application errors in an S3 Bucket. The engineers using these stack traces review them when addressing application issues. It has been decided that the files only need to be kept for four weeks then they can be purged. How can you meet this requirement in S3?

- ✓ Configure the S3 Lifecycle rules to purge the files after a month.
- ✗ Create a bucket policy to purge the rules after one month.
- ✗ Add an S3 Lifecycle rule to archive these files to Glacier after one month. Selected
- ✗ Write a cron job to purge the files after one month.

EXPLANATION

Incorrect - Archiving to Glacier would save some money, but does not meet the requirement of purging the files after one month.

Correct: To manage your objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

Transition actions define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

Expiration actions define when objects expire. Amazon S3 deletes expired objects on your behalf.

The lifecycle expiration costs depend on when you choose to expire objects.

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

QUESTION 19

Your company is slowly migrating to the cloud and is currently in a hybrid environment. The server team has been provisioning servers to their exact specifications using Chef recipes. These recipes can be reused in AWS. Which AWS services are designed to work with existing Chef recipes?

- ✗ AWS Systems Manager
- ✗ CloudFormation Selected
- ✓ Opsworks
- ✗ Elastic Beanstalk

EXPLANATION

Incorrect. OpsWorks is designed to work with Chef recipes.

AWS OpsWorks Stacks supports multiple versions of Chef. You select the version when you create the stack. AWS OpsWorks Stacks then installs that version of Chef on all of the stack's instances along with a set of built-in recipes that are compatible with that version. If you install any custom recipes, they must be compatible with the stack's Chef version. AWS OpsWorks Stacks currently supports Chef versions 12, 11.10, 11.4, and 0.9 for Linux stacks and Chef 12.2 (currently Chef 12.22) for Windows stacks. For convenience, they are usually referred to by just their major and minor version numbers. For Linux stacks, you can use the Configuration Manager to specify which Chef version to use when you create a stack. Windows stacks must use Chef 12.2. For more information, including guidelines for migrating stacks to more recent Chef versions, see Chef Versions.

QUESTION 20

After several issues with your application and unplanned downtime, your recommendation to migrate your application to AWS is approved. You have set up high availability on the front end with a load balancer and an Auto Scaling Group. What step can you take with your database to configure high-availability and ensure minimal downtime (under five minutes)?

- ✓ Enable Multi-AZ failover on the database. Selected
- ✗ Create a read replica.
- ✗ Create your database using CloudFormation and save the template for reuse.
- ✗ Take frequent snapshots of your database.

EXPLANATION

Correct. In the event of a planned or unplanned outage of your DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone if you have enabled Multi-AZ. The time it takes for the failover to complete depends on the database activity and other conditions at the time the primary DB instance became unavailable. Failover times are typically 60–120 seconds. However, large transactions or a lengthy recovery process can increase failover time. When the failover is complete, it can take additional time for the RDS console to reflect the new Availability Zone. Note the above sentences. Large transactions could cause a problem in getting back up within five minutes, but this is clearly the best of the available choices to attempt to meet this requirement. We must move through our questions on the exam quickly, but always evaluate all the answers for the best possible solution.

QUESTION 21

Several S3 Buckets have been deleted and a few EC2 instances have been terminated. Which AWS service can you use to determine who took these actions?

- ✗ AWS Inspector
- ✗ Trusted Advisor
- ✓ AWS CloudTrail Selected
- ✗ AWS CloudWatch

EXPLANATION

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

QUESTION 22

A car insurance company keeps specific details about accidents on file for a year, for quick retrieval, and then archives those files to long-term storage. A recent audit has approved the general steps they are taking, but pointed out many deficiencies in the technologies they are using. You have been hired as a consultant to come up with a solution. Your solution will recommend AWS storage options. What storage options could you recommend to meet the lifecycle requirements outlined, and provide high availability at a reasonable cost?

- ✗ Store the accident files in EBS volumes for a year, then migrate them to Glacier.
- ✗ Store the accident files in Glacier for maximum cost savings.
- ✗ Store the accident files in S3 for a year, then have the lifecycle policy move them to S3 IA
- ✓ Store the accident files in S3 for a year, then archive to Glacier. Selected

EXPLANATION

Correct: To manage your objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that defines actions that Amazon S3 applies to a group of objects. There are two types of actions:

Transition actions define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

Expiration actions define when objects expire. Amazon S3 deletes expired objects on your behalf.

The lifecycle expiration costs depend on when you choose to expire objects.

QUESTION 23

A small startup company has begun using AWS for all of its IT infrastructure. The company has one AWS Solutions Architect and the demands for his time are overwhelming. The software team has been given permission to deploy their Python and PHP applications on their own. They would like to deploy these applications without having to worry about the underlying infrastructure. Which AWS service would they use for deployments?

- ✗ CodeDeploy Selected
- ✗ CloudFront
- ✓ Elastic Beanstalk
- ✗ CloudFormation

EXPLANATION

Incorrect. CodeDeploy is more complex than Elastic Beanstalk and does not meet the ease of use requirements.

With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications. Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring. Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby. When you deploy your application, Elastic Beanstalk builds the selected supported platform version and provisions one or more AWS resources, such as Amazon EC2 instances, to run your application.
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html

QUESTION 24

You have just been hired by a large organization which uses many different AWS services in their environment. Some of the services which handle data include: RDS, Redshift, ElastiCache, DynamoDB, S3, and Glacier. You have been instructed to configure a web application using stateless web servers. Which services can you use to handle session state data? Choose two.

- ✓ DynamoDB Selected
- ✗ Glacier
- ✗ Redshift
- ✓ Elasticache Selected
- ✗ RDS

EXPLANATION

Elasticache and DynamoDB can both be used to store session data.
https://aws.amazon.com/caching/session-management/

https://docs.aws.amazon.com/sdk-for-net/v2/developer-guide/dynamodb-session-net-sdk.html

Elasticache and DynamoDB both can be used to store session data.
https://aws.amazon.com/caching/session-management/

https://docs.aws.amazon.com/sdk-for-net/v2/developer-guide/dynamodb-session-net-sdk.html

QUESTION 25

You have been given an assignment to configure Network ACLs in your VPC. Before configuring the NACLs, you need to understand how the NACLs are evaluated. How are NACL rules evaluated?

- ✗ All NACL rules that you configure are evaluated before traffic is passed through.
- ✗ NACL rules are evaluated by rule number from highest to lowest, and executed immediately when a matching rule is found.
- ✓ NACL rules are evaluated by rule number from lowest to highest and executed immediately when a matching rule is found. Selected
- ✗ NACL rules are evaluated by rule number from highest to lowest, and all are evaluated before traffic is passed through.

EXPLANATION

Correct. You can add or remove rules from the default network ACL, or create additional network ACLs for your VPC. When you add or remove rules from a network ACL, the changes are automatically applied to the subnets that it's associated with. 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. The following are the parts of a network ACL rule:

- Rule number. Rules are evaluated starting with the lowest-numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that might contradict it.
- Type. The type of traffic, for example, SSH. You can also specify all traffic or a custom range.
- Protocol. You can specify any protocol that has a standard protocol number. For more information, see Protocol Numbers. If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.
- Port range. The listening port or port range for the traffic. For example, 80 for HTTP traffic.
- Source. [Inbound rules only] The source of the traffic (CIDR range).
- Destination. [Outbound rules only] The destination for the traffic (CIDR range).
- Allow/Deny. Whether to allow or deny the specified traffic.

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

QUESTION 26

You have been assigned to create an architecture which uses load balancers to direct traffic to an Auto Scaling Group of EC2 instances across multiple Availability Zones. The application to be deployed on these instances is a life insurance application which requires path-based and host-based routing. Which type of load balancer will you need to use?

- ✗ Any type of load balancer will meet these requirements.
- ✗ Network Load Balancer
- ✗ Classic Load Balancer
- ✓ Application Load Balancer Selected

EXPLANATION

Correct. Only the Application Load Balancer can support path-based and host-based routing. Using an Application Load Balancer instead of a Classic Load Balancer has the following benefits:

- Support for path-based routing. You can configure rules for your listener that forward requests based on the URL in the request. This enables you to structure your application as smaller services, and route requests to the correct service based on the content of the URL.
- Support for host-based routing. You can configure rules for your listener that forward requests based on the host field in the HTTP header. This enables you to route requests to multiple domains using a single load balancer.
- Support for routing based on fields in the request, such as standard and custom HTTP headers and methods, query parameters, and source IP addresses.
- Support for routing requests to multiple applications on a single EC2 instance. You can register each instance or IP address with the same target group using multiple ports.
- Support for redirecting requests from one URL to another.
- Support for returning a custom HTTP response.
- Support for registering targets by IP address, including targets outside the VPC for the load balancer.
- Support for registering Lambda functions as targets.
- Support for the load balancer to authenticate users of your applications through their corporate or social identities before routing requests.
- Support for containerized applications. Amazon Elastic Container Service (Amazon ECS) can select an unused port when scheduling a task and register the task with a target group using this port. This enables you to make efficient use of your clusters.
- Support for monitoring the health of each service independently, as health checks are defined at the target group level and many CloudWatch metrics are reported at the target group level. Attaching a target group to an Auto Scaling group enables you to scale each service dynamically based on demand.
- Access logs contain additional information and are stored in compressed format.
- Improved load balancer performance.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html#application-load-balancer-benefits https://aws.amazon.com/elasticloadbalancing/faqs/

QUESTION 27

The CFO of your company approaches you and inquires about cutting costs in your AWS account. One area you are able to identify for cost cutting is in S3. There is data in S3 that is very rarely used and has only been retained for audit purposes. You decide to archive this data to a cheaper storage solution. Which AWS solution would meet this requirement?

- ✓ Use a lifecycle policy to archive the data to Glacier. Selected
- ✗ Use a lifecycle policy to archive the data to Amazon SQS.
- ✗ Use a lifecycle policy to archive the data to Redshift.
- ✗ Write a cron job to archive the data to DynamoDB.

EXPLANATION

Correct: Using S3 Lifecycle configuration, you can transition objects to the S3 Glacier or S3 Glacier Deep Archive storage classes for archiving. When you choose the S3 Glacier or S3 Glacier Deep Archive storage class, your objects remain in Amazon S3. You cannot access them directly through the separate Amazon S3 Glacier service.
https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

QUESTION 28

You have a typical architecture of an Application Load Balancer fronting an Auto Scaling Group of EC2 instances, backed by an RDS MySQL database. Your Application Load Balancer is performing health checks on the EC2 instances. What actions will be taken if an instance fails these health checks?

- ✗ The instance is replaced by the ALB.
- ✓ The ALB stops sending traffic to the instance. Selected
- ✗ The ALB notifies the Auto Scaling Group that the instance is down.
- ✗ The instance is terminated by the ALB.

EXPLANATION

Correct. The load balancer routes requests only to the healthy instances. When the load balancer determines that an instance is unhealthy, it stops routing requests to that instance. The load balancer resumes routing requests to the instance when it has been restored to a healthy state.
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html

QUESTION 29

You have been tasked with designing a strategy for backing up EBS volumes attached to an instance-store-backed EC2 instance. You have been asked for an executive summary on your design, and the executive summary should include an answer to the question, "What can an EBS volume do when snapshotting the volume is in progress"?

- ✗ The volume can only accommodate writes while a snapshot is in progress.
- ✓ The volume can be used normally while the snapshot is in progress.
- ✗ The volume can only accommodate reads while a snapshot is in progress. Selected
- ✗ The volume can not be used while a snapshot is in progress.

EXPLANATION

Incorrect. You can do everything, including reads, while a snapshot is in progress.

Correct. You can create a point-in-time snapshot of an EBS volume and use it as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental; the new snapshot saves only the blocks that have changed since your last snapshot. Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html

QUESTION 30

A travel company has deployed a website which serves travel updates to users all over the world. The traffic this database serves is very read heavy and can have some latency issues at certain times of the year. What can you do to alleviate these latency issues?

- ✓ Add read replicas Selected
- ✗ Place CloudFront in front of the Database.
- ✗ Configure multi-Region RDS
- ✗ Configure RDS Multi-AZ

EXPLANATION

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.
https://aws.amazon.com/rds/features/read-replicas/

QUESTION 31

Your organization uses AWS CodeDeploy for deployments. Now you are starting a project on the AWS Lambda platform. For your deployments, you've been given a requirement of performing blue-green deployments. When you perform deployments, you want to split traffic, sending a small percentage of the traffic to the new version of your application. Which deployment configuration will allow this splitting of traffic?

- ✓ Canary
- ✗ Linear
- ✗ Weighted routing Selected
- ✗ All at Once

EXPLANATION

Incorrect. Weighted routing does enable you to split traffic by percentage, but it is not a Lambda deployment configuration. Weighted routing is related to Route 53.

Correct. With canary, traffic is shifted in two increments. You can choose from predefined canary options that specify the percentage of traffic shifted to your updated Lambda function version in the first increment and the interval, in minutes, before the remaining traffic is shifted in the second increment.

https://docs.aws.amazon.com/codedeploy/latest/userguide/welcome.html#blue-green-lambda-compute-type

QUESTION 32

Your company has decided to migrate a SQL Server database to a newly-created AWS account. Which service can be used to migrate the database?

- ✓ Database Migration Service — Selected
- ✗ DynamoDB
- ✗ Elasticache
- ✗ AWS RDS

EXPLANATION

Correct. AWS Database Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from the most widely used commercial and open-source databases.

AWS Database Migration Service supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle or Microsoft SQL Server to Amazon Aurora. With AWS Database Migration Service, you can continuously replicate your data with high availability and consolidate databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift and Amazon S3. Learn more about the supported source and target databases.

https://aws.amazon.com/dms/

QUESTION 33

You are working for a large financial institution and preparing for disaster recovery and upcoming DR drills. A key component in the DR plan will be the database instances and their data. An aggressive Recovery Time Objective (RTO) dictates that the database needs to be synchronously replicated. Which configuration can meet this requirement?

- ✗ AWS Lambda to trigger a CloudFormation template launch in another Region.
- ✗ RDS read replicas
- ✓ RDS Multi-AZ
- ✗ RDS Multi-Region Selected

EXPLANATION

RDS Multi-Region does not exist. RDS Multi-AZ provides failover capability and synchronous replication.

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

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

QUESTION 34

You have been assigned to create an architecture which uses load balancers to direct traffic to an Auto Scaling Group of EC2 instances across multiple Availability Zones. You were considering using an Application Load Balancer, but some of the requirements you have been given seem to point to a Classic Load Balancer. Which requirement would be better served by an Application Load Balancer?

- ✗ Support for EC2-Classic
- ✓ Path-based routing
- ✗ Support for TCP and SSL listeners Selected
- ✗ Support for sticky sessions using application-generated cookies

EXPLANATION

Incorrect. This is a benefit of using a Classic Load Balancer.

Using an Application Load Balancer instead of a Classic Load Balancer has the following benefits:

Using an Application Load Balancer instead of a Classic Load Balancer has the following benefits:

- Support for path-based routing. You can configure rules for your listener that forward requests based on the URL in the request. This enables you to structure your application as smaller services, and route requests to the correct service based on the content of the URL.
- Support for host-based routing. You can configure rules for your listener that forward requests based on the host field in the HTTP header. This enables you to route requests to multiple domains using a single load balancer.
- Support for routing based on fields in the request, such as standard and custom HTTP headers and methods, query parameters, and source IP addresses.
- Support for routing requests to multiple applications on a single EC2 instance. You can register each instance or IP address with the same target group using multiple ports.
- Support for redirecting requests from one URL to another.
- Support for returning a custom HTTP response.
- Support for registering targets by IP address, including targets outside the VPC for the load balancer.
- Support for registering Lambda functions as targets.
- Support for the load balancer to authenticate users of your applications through their corporate or social identities before routing requests.
- Support for containerized applications. Amazon Elastic Container Service (Amazon ECS) can select an unused port when scheduling a task and register the task with a target group using this port. This enables you to make efficient use of your clusters.
- Support for monitoring the health of each service independently, as health checks are defined at the target group level and many CloudWatch metrics are reported at the target group level. Attaching a target group to an Auto Scaling Group enables you to scale each service dynamically based on demand.
- Access logs contain additional information and are stored in compressed format.
- Improved load balancer performance.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html

QUESTION 35

You are designing an architecture for a financial company which provides a day trading application to customers. After viewing the traffic patterns for the existing application you notice that traffic is fairly steady throughout the day, with the exception of large spikes at the opening of the market in the morning and at closing around 3 pm. Your architecture will include an Auto Scaling Group of EC2 instances. How can you configure the Auto Scaling Group to ensure that system performance meets the increased demands at opening and closing of the market?

- ✗ Configure a Dynamic Scaling Policy to scale based on CPU Utilization. Selected
- ✗ Use a load balancer to ensure that the load is distributed evenly during high-traffic periods.
- ✗ Configure your Auto Scaling Group to have a desired size which will be able to meet the demands of the high-traffic periods.
- ✓ Use a predictive scaling policy on the Auto Scaling Group to meet opening and closing spikes.

EXPLANATION

Incorrect. Although this may work, it is not the best solution available. While CPU Utilization is the most common metric to scale on, it is not always the best. A custom metric for memory utilization is often a better option. The question is not giving enough information to make Dynamic Scaling the best choice.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

Correct. Using data collected from your actual EC2 usage and further informed by billions of data points drawn from our own observations, we use well-trained Machine Learning models to predict your expected traffic (and EC2 usage) including daily and weekly patterns. The model needs at least one day's of historical data to start making predictions; it is re-evaluated every 24 hours to create a forecast for the next 48 hours. What we can gather from the question is that the spikes at the beginning and end of day can potentially affect performance. Sure, we can use dynamic scaling, but remember, scaling up takes a little bit of time. We have the information to be proactive, use predictive scaling, and be ready for these spikes at opening and closing.
https://aws.amazon.com/blogs/aws/new-predictive-scaling-for-ec2-powered-by-machine-learning/

QUESTION 36

You have been evaluating the NACLS in your company. Most of the NACLs are configured the same: 100 All Traffic Allow 200 All Traffic Deny '' *All Traffic Deny What function does the* '' rule perform?

- ✗ It is there in case no other rules are defined.
- ✓ This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied.
- ✗ The * specifies that it is an example rule. Selected
- ✗ Traffic will be denied from specified IP addresses.

EXPLANATION

Incorrect. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied.

The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated. Each network ACL also includes a rule whose rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule. https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

QUESTION 37

Your company is using a hybrid configuration because there are some legacy applications which are not easily converted and migrated to AWS. And with this configuration comes a typical scenario where the legacy apps must maintain the same private IP address and MAC address. You are attempting to convert the application to the cloud and have configured an EC2 instance to house the application. What you are currently testing is removing the ENI from the legacy instance and attaching it to the EC2 instance. You want to attempt a cold attach. What does this mean?

- ✗ Attach ENI when it's stopped. Selected
- ✗ Attach ENI to an instance when it's running.
- ✗ Attach ENI before the public IP address is assigned.
- ✓ Attach ENI when the instance is being launched.

EXPLANATION

Incorrect. This is known as a warm attach.

EXPLANATION

Incorrect. This is known as a warm attach.

Best practices for configuring network interfaces You can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach). You can detach secondary network interfaces when the instance is running or stopped. However, you can't detach the primary network interface. You can move a network interface from one instance to another, if the instances are in the same Availability Zone and VPC but in different subnets. When launching an instance using the CLI, API, or an SDK, you can specify the primary network interface and additional network interfaces. Launching an Amazon Linux or Windows Server instance with multiple network interfaces automatically configures interfaces, private IPv4 addresses, and route tables on the operating system of the instance. A warm or hot attach of an additional network interface may require you to manually bring up the second interface, configure the private IPv4 address, and modify the route table accordingly. Instances running Amazon Linux or Windows Server automatically recognize the warm or hot attach and configure themselves. Attaching another network interface to an instance (for example, a NIC teaming configuration) cannot be used as a method to increase or double the network bandwidth to or from the dual-homed instance. If you attach two or more network interfaces from the same subnet to an instance, you may encounter networking issues such as asymmetric routing. If possible, use a secondary private IPv4 address on the primary network interface instead. For more information, see Assigning a secondary private IPv4 address. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 38

You have recently migrated your small company to AWS and are looking for some general best practice guidance within the platform. Which AWS service can help you optimize your AWS environment by giving recommendations to reduce cost, increase security, and improve performance.

- ✗ AWS Inspector
- ✗ AWS Optimizations
- ✗ AWS Organizations
- ✓ AWS Trusted Advisor Selected

EXPLANATION

Correct: AWS Trusted Advisor is an online tool that provides you realtime guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits. Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

QUESTION 39

You are working as a Solutions Architect for an online travel company. Your application is going to use an Auto Scaling Group of EC2 instances but you need to have some decoupling to store messages because of high volume. Which AWS service can be added to the solution that can meet this requirement?

- ✗ RDS Read Replicas
- ✗ Elasticache
- ✓ AWS SQS Selected
- ✗ AWS Simple Workflow Service

EXPLANATION

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface, or SDK of your choice, and three simple commands. SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.
https://aws.amazon.com/sqs/

QUESTION 40

Your company has recently converted to a hybrid cloud environment and will slowly be migrating to a fully AWS cloud environment. The AWS side is in need of some steps to prepare for disaster recovery. A disaster recovery plan needs drawn up and disaster recovery drills need to be performed for compliance reasons. The company wants to establish Recovery Time and Recovery Point Objectives. The RTO and RPO can be pretty relaxed. The main point is to have a plan in place, with as much cost savings as possible. Which AWS disaster recovery pattern will best meet these requirements?

- ✓ Backup and restore Selected
- ✗ Warm Standby
- ✗ Multi Site
- ✗ Pilot Light

EXPLANATION

Correct: This is the least expensive option and cost is the overriding factor.

QUESTION 41

You work for an oil and gas company as a lead in data analytics. The company is using IoT devices to better understand their assets in the field (for example, pumps, generators, valve assemblies, and so on). Your task is to monitor the IoT devices in real-time to provide valuable insight that can help you maintain the reliability, availability, and performance of your IoT devices. What tool can you use to process streaming data in real time with standard SQL without having to learn new programming languages or processing frameworks?

- ✗ AWS Lambda
- ✗ AWS RedShift
- ✓ Kinesis Data Analytics
- ✗ AWS Kinesis Streams Selected

EXPLANATION

Incorrect. Kinesis Streams can stream data real-time, but Kinesis Data Analytics is designed to meet this requirement.

Monitoring IoT devices in real-time can provide valuable insight that can help you maintain the reliability, availability, and performance of your IoT devices. You can track time series data on device connectivity and activity. This insight can help you react quickly to changing conditions and emerging situations. Amazon Web Services (AWS) offers a comprehensive set of powerful, flexible, and simple-to-use services that enable you to extract insights and actionable information in real time. Amazon Kinesis is a platform for streaming data on AWS, offering key capabilities to cost-effectively process streaming data at any scale. Kinesis capabilities include Amazon Kinesis Data Analytics, the easiest way to process streaming data in real time with standard SQL without having to learn new programming languages or processing frameworks. https://docs.aws.amazon.com/solutions/latest/real-time-iot-device-monitoring-with-kinesis/overview.html

QUESTION 42

A team member has been tasked to configure four EC2 instances for four separate applications. These are not high-traffic apps, so there is no need for an Auto Scaling Group. The instances are all in the same public subnet and each instance has an EIP address, and all of the instances have the same Security Group. But none of the instances can send or receive internet traffic. You verify that all the instances have a public IP address. You also verify that an internet gateway has been configured. What is the most likely issue?

- ✓ There is no route in the route table to the internet gateway (or it has been deleted). Selected
- ✗ You are using the default nacl.
- ✗ The route table is corrupt.
- ✗ Each instance needs its own security group.

EXPLANATION

The question details all of the configuration needed for internet access, except for a route to the IGW in the route table. This is definitely a key step in any checklist for internet connectivity. It is quite possible to have a subnet with the 'Public' attribute set but no route to the Internet in the assigned Route table. (test it yourself). This may have been a setup error, or someone may have thoughtlessly altered the shared Route table for a special case instead of creating a new Route table for the special case.

- https://docs.aws.amazon.com/AmazonECS/latest/developerguide/create-public-private-vpc.html

QUESTION 43

A new startup company decides to use AWS to host their web application. They configure a VPC as well as two subnets within the VPC. They also attach an internet gateway to the VPC. In the first subnet, they create an EC2 instance to host a web application. There is a network ACL and a security group, which both have the proper ingress and egress to and from the internet. There is a route in the route table to the internet gateway. The EC2 instances added to the subnet need to have a globally unique IP address to ensure internet access. Which is not a globally unique IP address?

- ✓ private IP address
- ✗ elastic IP address Selected
- ✗ IPv6 address
- ✗ public IP address

EXPLANATION

Incorrect. This is a globally unique address.

Correct. To enable access to or from the Internet for instances in a subnet in a VPC, you must do the following: Attach an internet gateway to your VPC. Add a route to your subnet's route table that directs internet-bound traffic to the internet gateway. If a subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet. If a subnet is associated with a route table that does not have a route to an internet gateway, it's known as a private subnet. Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, elastic IP address, or IPv6 address). Ensure that your network access control lists and security group rules allow the relevant traffic to flow to and from your instance.

QUESTION 44

You have been assigned to migrate an application and the servers it runs on to the company AWS cloud environment. You have created a checklist of steps necessary to perform this migration. A subsection in the checklist is security considerations. One of the things that you need to consider is the shared responsibility module. Which option does the customer handle under the shared responsibility model?

- ✗ Network infrastructure
- ✗ Hardware infrastructure
- ✓ Identity and Access Management Selected
- ✗ Availability Zones

EXPLANATION

Identity and Access Management is the responsibility of the customer. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions. https://aws.amazon.com/compliance/shared-responsibility-model/

QUESTION 45

A software company has produced several stateless applications. The software team now needs servers to act as test servers for these applications. These servers are not mission-critical, so occasional downtime is acceptable. What type of EC2 servers can be used to meet these requirements at the lowest cost?

- ✗ Dedicated Hosts
- ✓ Spot Selected
- ✗ Reserved
- ✗ On-Demand

EXPLANATION

You can use Spot Instances for various fault-tolerant and flexible applications. Examples include web servers, API backends, continuous integration/continuous development, and Hadoop data processing.

You can also take advantage of Spot Instances to run and scale applications such as stateless web services, image rendering, big data analytics, and massively parallel computations. Spot Instances are typically used to supplement On-Demand Instances, where appropriate, and are not meant to handle 100% of your workload. However, you can use all Spot Instances for any stateless, non-production application, such as development and test servers, where occasional downtime is acceptable. They are not a good choice for sensitive workloads or databases.

https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-leveraging-ec2-spot-instances/when-to-use-spot-instances.html

QUESTION 46

A consultant hired by a small company to configure an AWS environment. The consultant begins working with the VPC and launching EC2 instances within the VPC. The initial instances will be placed in a public subnet. The consultant begins to create security groups. What is true of security groups?

- ✓ You can specify allow rules but not deny rules. Selected
- ✗ You can specify deny rules, but not allow rules.
- ✗ By default, a security group includes an inbound rule that allows all inbound traffic.
- ✗ You can't specify separate rules for inbound and outbound traffic.

EXPLANATION

The following are the basic characteristics of security groups for your VPC: There are quotas on the number of security groups that you can create per VPC, the number of rules that you can add to each security group, and the number of security groups that you can associate with a network interface. For more information, see Amazon VPC quotas. You can specify allow rules, but not deny rules. You can specify separate rules for inbound and outbound traffic. When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group. By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed. Security groups are stateful. If you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

QUESTION 47

You are put in charge of your company's Disaster Recovery planning. As part of this plan, you intend to create all of the company infrastructure with CloudFormation templates. The templates can then be saved in another region and used to launch a new environment in case of disaster. What determines the costs associated with CloudFormation templates?

- ✗ It depends whether the resources in the template are in the free tier.
- ✗ The distance of the region from the home region.
- ✓ There is no cost for templates, but when deployed, the resources created will accumulate charges.
- ✗ There is a cost per template and discounts for over 100 templates.

EXPLANATION

Correct: There is no additional charge for using AWS CloudFormation with resource providers in the following namespaces: AWS::, *Alexa::*, and Custom::*. In this case you pay for AWS resources (such as Amazon EC2 instances, Elastic Load Balancing load balancers, etc.) created using AWS CloudFormation as if you created them manually. You only pay for what you use, as you use it; there are no minimum fees and no required upfront commitments. When you use resource providers with AWS CloudFormation outside the namespaces mentioned above, you incur charges per handler operation. Handler operations are create, update, delete, read, or list actions on a resource.

https://aws.amazon.com/cloudformation/pricing/

QUESTION 48

A small software team is creating an application which will give subscribers real-time weather updates. The application will run on EC2 and will make several requests to AWS services such as S3 and DynamoDB. What is the best way to grant permissions to these other AWS services?

- ✗ Create an IAM policy that you attach to the EC2 instance to give temporary security credentials to applications running on the instance. Selected
- ✗ Create an IAM user, grant the user permissions, and pass the user credentials to the application.
- ✓ Create an IAM role that you attach to the EC2 instance to give temporary security credentials to applications running on the instance.
- ✗ Embed the appropriate credentials to access AWS services in the application.

EXPLANATION

Incorrect. There will be a policy which grants the proper permissions. But a policy attaches to a role, and then the role can be attached to the EC2 instance when the instance is launched.

Create an IAM role in the following situations: You're creating an application that runs on an Amazon Elastic Compute Cloud (Amazon EC2) instance and that application makes requests to AWS. Don't create an IAM user and pass the user's credentials to the application or embed the credentials in the application. Instead, create an IAM role that you attach to the EC2 instance to give temporary security credentials to applications running on the instance. When an application uses these credentials in AWS, it can perform all of the operations that are allowed by the policies attached to the role. For details, see Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances.

QUESTION 49

You have been tasked with migrating an application and the servers it runs on to the company AWS cloud environment. You have created a checklist of steps necessary to perform this migration. A subsection in the checklist is security considerations. One of the things that you need to consider is the shared responsibility module. Which option does AWS handle under the shared responsibility model?

- ✗ Client-side data encryption
- ✗ User Authentication
- ✗ Firewall Configuration
- ✓ Physical Hardware Infrastructure Selected

EXPLANATION

Security and compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility for, and management of, the guest operating system (including updates and security patches), other associated application software, and the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose, as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud.

AWS responsibility "Security of the Cloud": AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

QUESTION 50

An insurance company is creating an application which will perform analytics in near real-time on huge datasets in the terabyte range and potentially even petabyte. The company is evaluating an AWS data storage option. Which AWS service will allow storage of petabyte scale data and also allow fast querying of this data?

- ✗ DynamoDb
- ✓ Redshift Selected
- ✗ ElastiCache
- ✗ RDS

EXPLANATION

Correct. Amazon Redshift is a fully-managed, petabyte-scale data warehouse service in the Cloud. An Amazon Redshift data warehouse is a collection of computing resources called nodes, which are organized into a group called a cluster. Each cluster runs an Amazon Redshift engine and contains one or more databases.
https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html

https://docs.aws.amazon.com/redshift/latest/gsg/getting-started.html

QUESTION 51

A company has a great deal of data in S3 buckets for which they want to create a database. Creating the RDS database, normalizing the data, and migrating to the RDS database will take time and is the long-term plan. But there's an immediate need to query this data to retrieve information necessary for an audit. Which AWS service will enable querying data in S3 using standard SQL commands?

- ✗ Amazon SQL Connector
- ✓ Amazon Athena Selected
- ✗ There is no such service, but there are third-party tools.
- ✗ DynamoDB

EXPLANATION

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you only pay for the queries you run.

Athena is easy to use. Simply point to your data in Amazon S3, define the schema, and start querying using standard SQL. Most results are delivered within seconds. With Athena, there's no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets. https://aws.amazon.com/athena/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

QUESTION 52

A consultant is hired by a small company to configure an AWS environment. The consultant begins working with the VPC and launching EC2 instances within the VPC. The initial instances will be placed in a public subnet. The consultant begins to create security groups. The consultant has launched several instances, created security groups, and has associated security groups with instances. The consultant wants to change the security groups for an instance. Which statement is true?

- ✗ You can't change security groups. Create a new instance and attach the desired security groups.
- ✗ You can change the security groups for an instance when the instance is in the pending or stopped state.
- ✗ You can't change the security groups for an instance when the instance is in the running or stopped state.
- ✓ You can change the security groups for an instance when the instance is in the running or stopped state. Selected

EXPLANATION

Correct. After you launch an instance into a VPC, you can change the security groups that are associated with the instance. You can change the security groups for an instance when the instance is in the running or stopped state.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

QUESTION 53

Your company has asked you to look into some latency issues with the company web app. The application is backed by an AWS RDS database. Your analysis has determined that the requests made of the application are very read heavy, and this is where improvements can be made. Which service can you use to store frequently accessed data in-memory?

- ✓ ElastiCache Selected
- ✗ EBS
- ✗ DynamoDB
- ✗ DAX

EXPLANATION

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases. There are two types of ElastiCache available: Memcached and Redis. Here is a good overview and comparison between them: https://aws.amazon.com/elasticache/redis-vs-memcached/

QUESTION 54

A consultant is hired by a small company to configure an AWS environment. The consultant begins working with the VPC and launching EC2 instances within the VPC. The initial instances will be placed in a public subnet. The consultant begins to create security groups. What is true of the default security group?

- ✗ You can't delete this group, nor can you change the group's rules.
- ✗ You can delete this group or you can change the group's rules.
- ✓ You can't delete this group, however, you can change the group's rules.
- ✗ You can delete this group, however, you can't change the group's rules. Selected

EXPLANATION

Incorrect. You cannot delete this group.

Your VPC includes a default security group. You can't delete this group, however, you can change the group's rules. The procedure is the same as modifying any other security group. For more information, see Adding, removing, and updating rules.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

QUESTION 55

A data company has implemented a subscription service for storing video files. There are two levels of subscription: personal and professional use. The personal users can upload a total of 5 GB of data, and professional users can upload as much as 5 TB of data. The application can upload files of size up to 1 TB to an S3 Bucket. What is the best way to upload files of this size?

- ✗ AWS SnowMobile
- ✓ Multipart upload Selected
- ✗ AWS Snowball
- ✗ Single-part Upload

EXPLANATION

The Multipart upload API enables you to upload large objects in parts. You can use this API to upload new large objects or make a copy of an existing object (see Operations on Objects). Multipart uploading is a three-step process: You initiate the upload, you upload the object parts, and after you have uploaded all the parts, you complete the multipart upload. Upon receiving the complete multipart upload request, Amazon S3 constructs the object from the uploaded parts, and you can then access the object just as you would any other object in your bucket. You can list all of your in-progress multipart uploads or get a list of the parts that you have uploaded for a specific multipart upload. Each of these operations is explained in this section.
https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html

QUESTION 56

A financial institution has an application that produces huge amounts of actuary data, which is ultimately expected to be in the terabyte range. There is a need to run complex analytic queries against terabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution. Which storage service will best meet this requirement?

- ✗ Elasticache
- ✓ Redshift Selected
- ✗ DynamoDB
- ✗ RDS

EXPLANATION

Amazon Redshift is a fast, fully-managed cloud data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It enables you to run complex analytic queries against terabytes to petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution. Most results come back in seconds. With Redshift, you can start small for just $0.25 per hour with no commitments and scale-out to petabytes of data for $1,000 per terabyte per year, less than a tenth of the cost of traditional on-premises solutions. Amazon Redshift also includes Amazon Redshift Spectrum, allowing you to run SQL queries directly against exabytes of unstructured data in Amazon S3 data lakes. No loading or transformation is required, and you can use open data formats, including Avro, CSV, Grok, Amazon Ion, JSON, ORC, Parquet, RCFile, RegexSerDe, Sequence, Text, and TSV. Redshift Spectrum automatically scales query compute capacity based on the data retrieved, so queries against Amazon S3 run fast, regardless of data set size.

QUESTION 57

You have configured a VPC with both a public and a private subnet. You need to deploy a web server and a database. You want the web server to be accessed from the Internet by customers. Which is the proper configuration for this architecture?

- ✗ Database outside the VPC for decoupling from web server, and web server in public subnet for internet access.
- ✓ Web server in public subnet, database in private subnet. Selected
- ✗ Web server outside of VPC for internet access, database in private subnet.
- ✗ Both web server and database in public subnets to facilitate internet access.

EXPLANATION

Correct. In a best-practice VPC architecture, you launch the web servers or elastic load balancers in the public subnet and the database servers in the private subnet.
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

QUESTION 58

You have configured an Auto Scaling Group of EC2 instances. You have begun testing the scaling of the Auto Scaling Group using a stress tool to force the CPU utilization metric being used to force scale out actions. The stress tool is also being manipulated by removing stress to force a scale in. But you notice that these actions are only taking place in five-minute intervals. What is happening?

- ✗ A load balancer is managing the load and limiting the effectiveness of stressing the servers.
- ✗ Auto Scaling Groups can only scale in intervals of five minutes or greater. Selected
- ✗ The stress tool is configured to run for five minutes.
- ✓ The Auto Scaling Group is following the default cooldown procedure.

EXPLANATION

Incorrect. This interval is configurable and can be less than five minutes.

The cooldown period helps you prevent your Auto Scaling group from launching or terminating additional instances before the effects of previous activities are visible. You can configure the length of time based on your instance startup time or other application needs. When you use simple scaling, after the Auto Scaling group scales using a simple scaling policy, it waits for a cooldown period to complete before any further scaling activities due to simple scaling policies can start. An adequate cooldown period helps to prevent the initiation of an additional scaling activity based on stale metrics. By default, all simple scaling policies use the default cooldown period associated with your Auto Scaling Group, but you can configure a different cooldown period for certain policies, as described in the following sections. Note that Amazon EC2 Auto Scaling honors cooldown periods when using simple scaling policies, but not when using other scaling policies or scheduled scaling. A default cooldown period automatically applies to any scaling activities for simple scaling policies, and you can optionally request to have it apply to your manual scaling activities. When you use the AWS Management Console to update an Auto Scaling Group, or when you use the AWS CLI or an AWS SDK to create or update an Auto Scaling Group, you can set the optional default cooldown parameter. If a value for the default cooldown period is not provided, its default value is 300 seconds.

QUESTION 59

After an IT Steering Committee meeting, you have been put in charge of configuring a hybrid environment for the company's compute resources. You weigh the pros and cons of various technologies, such as VPN and Direct Connect, and based on the requirements you have decided to configure a VPN connection. What features and advantages can a VPN connection provide?

- ✓ It provides a connection between an on-premises network and a VPC, using a secure and private connection with IPsec and TLS. Selected
- ✗ It provides a private, dedicated network connection between an on-premises network and the VPC.
- ✗ It provides a network connection between two VPCs that can route traffic using IPv4 or IPv6.
- ✗ It provides a cost-effective, private network connection that bypasses the internet.

EXPLANATION

Correct: A VPC/VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low-to-modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources or your on-premises network. With AWS Client VPN, you configure an endpoint to which your users can connect to establish a secure TLS VPN session. This enables clients to access resources in AWS or on-premises from any location using an OpenVPN-based VPN client.

You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the Site-to-Site VPN connection, a virtual private gateway or transit gateway provides two VPN endpoints (tunnels) for automatic failover. You configure your customer gateway device on the remote side of the Site-to-Site VPN connection.

https://docs.aws.amazon.com/vpc/latest/userguide/vpn-connections.html

QUESTION 60

A database outage has been very costly to your organization. You have been tasked with configuring a more highly-available architecture. The main requirement is that the chosen architecture needs to meet an aggressive RTO in case of disaster. You have decided to use an RDS Multi-AZ deployment. How is the replication handled for RDS Multi-AZ?

- ✗ Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Region.
- ✓ Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. Selected
- ✗ Amazon RDS automatically provisions and maintains an asynchronous standby replica in a different Availability Zone.
- ✗ You can configure a standby replica in a different Availability Zone and send traffic synchronously or asynchronously depending on your cost considerations.

EXPLANATION

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. Multi-AZ deployments for MariaDB, MySQL, Oracle, and PostgreSQL DB instances use Amazon's failover technology. SQL Server DB instances use SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs). In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

QUESTION 61

A small company has nearly 200 users who already have AWS accounts in the company AWS environment. A new S3 bucket has been created which will allow roughly a third of all users access to sensitive information in the bucket. What is the most time efficient way to get these users access to the bucket?

- ✗ Create a new bucket policy granting the appropriate permissions and attach it to the bucket.
- ✓ Create a new policy which will grant permissions to the bucket. Create a group and attach the policy to that group. Add the users to this group. Selected
- ✗ Create a new role which will grant permissions to the bucket. Create a group and attach the role to that group. Add the users to this group.
- ✗ Create a new policy which will grant permissions to the bucket. Create a role and attach the policy to that role. Add the users to this role.

EXPLANATION

An IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, you could have a group called Admins and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to the group. If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to that group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old groups and add him or her to the appropriate new groups. Note that a group is not truly an "identity" in IAM because it cannot be identified as a Principal in a permission policy. It is simply a way to attach policies to multiple users at one time. Following are some important characteristics of groups:

- A group can contain many users, and a user can belong to multiple groups.
- Groups can't be nested; they can contain only users, not other groups.
- There's no default group that automatically includes all users in the AWS account. If you want to have a group like that, you need to create it and assign each new user to it.
- There's a limit to the number of groups you can have, and a limit to how many groups a user can be in. For more information, see IAM and STS Limits.

QUESTION 62

An international travel company has an application which provides travel information and alerts to users all over the world. The application is hosted on groups of EC2 instances in Auto Scaling Groups in multiple AWS Regions. There are also load balancers routing traffic to these instances. In two countries, Ireland and Australia, there are compliance rules in place that dictate users connect to the application in eu-west-1 and ap-southeast-1. Which service can you use to meet this requirement?

- ✗ Configure CloudFront and the users will be routed to the nearest edge location.
- ✗ Use Route 53 weighted routing.
- ✓ Use Route 53 geolocation routing. Selected
- ✗ Configure the load balancers to route users to the proper region.

EXPLANATION

Correct. Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB in the Frankfurt region. When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights. Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.

QUESTION 63

A consultant hired by a small company to configure an AWS environment. The consultant begins working with the VPC and launching EC2 instances within the VPC. The initial instances will be placed in a public subnet. The consultant begins to create security groups. What is true of security groups?

- ✓ Security groups act at the instance level, not the subnet level.
- ✗ Security groups act at the subnet level, not the instance level.
- ✗ Security groups act at the VPC level, not the instance level. Selected
- ✗ Security groups are stateless.

EXPLANATION

Incorrect. Security groups act at the instance level.

The following are the basic characteristics of security groups for your VPC:

- There are quotas on the number of security groups that you can create per VPC, the number of rules that you can add to each security group, and the number of security groups that you can associate with a network interface. For more information, see Amazon VPC quotas.
- You can specify allow rules, but not deny rules.
- You can specify separate rules for inbound and outbound traffic.
- When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
- By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.
- Security groups are stateful. If you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

QUESTION 64

A new startup company decides to use AWS to host their web application. They configure a VPC as well as two subnets within the VPC. They also attach an internet gateway to the VPC. In the first subnet, they create the EC2 instance which will host their web application. They finish the configuration by making the application accessible from the Internet. The second subnet has an instance hosting a smaller, secondary application. But this application is not currently accessible from the Internet. What could be potential problems?

- ✓ The second subnet does not have a route in the route table to the internet gateway. Selected
- ✗ The second subnet does not have a route in the route table to the virtual private gateway. Selected
- ✓ The EC2 instance does not have a public IP address.
- ✗ The EC2 instance is not attached to an internet gateway.
- ✗ The second subnet does not have a public IP address.

EXPLANATION

Incorrect. Virtual private gateways are not used for internet access.

To enable access to or from the internet for instances in a subnet in a VPC, you must do the following:

- Attach an internet gateway to your VPC.
- Add a route to your subnet's route table that directs internet-bound traffic to the internet gateway. If a subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet. If a subnet is associated with a route table that does not have a route to an internet gateway, it's known as a private subnet.
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control lists and security group rules allow the relevant traffic to flow to and from your instance.

QUESTION 65

The AWS team in a large company is spending a lot of time monitoring EC2 instances and maintenance when the instances report health check failures. How can you most efficiently automate this monitoring and repair?

- ✗ Create a Lambda function which can be triggered by a failed instance health check. Have the Lambda function destroy the instance and spin up a new instance.
- ✗ Create a Lambda function which can be triggered by a failed instance health check. Have the Lambda function deploy a CloudFormation template which can perform the creation of a new instance.
- ✗ Create a cron job which monitors the instances periodically and starts a new instance if a health check has failed.
- ✓ Create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically reboots the instance if a health check fails. Selected

EXPLANATION

You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically reboots the instance. The reboot alarm action is recommended for Instance Health Check failures (as opposed to the recover alarm action, which is suited for System Health Check failures). An instance reboot is equivalent to an operating system reboot. In most cases, it takes only a few minutes to reboot your instance. When you reboot an instance, it remains on the same physical host, so your instance keeps its public DNS name, private IP address, and any data on its instance store volumes. Rebooting an instance doesn't start a new instance billing hour, unlike stopping and restarting your instance.