

1) A developer needs to be notified by email for all new object creation events in a specific amazon s3 bucket. Amazon sns will be used for sending the messages. How can the developer enable these notifications?

Ans: **create an event notification for all s3 object created* api calls (option b)**

2) you are a solutions architect for a multinational law firm based in london. Their operations are worldwide and they have several VPCs in the US, europe and asia regions. As part of the internal infra audit, your CTO wants to set up a single dashboard to collectively monitor all of the firm's EC2 instances which are located in different Aws regions. Which of the following is the best option that will meet the requirement

Ans: **Monitoring aws resources in multiple regions can be simply done using a single cloudwatch dashboard**

3) A company has on-premises servers running a relational database . The current database serves high read traffic for users in different locations. The company wants to migrate to aws with the least amount of effort. The database solution should support disaster recovery

Ans: **use a database in amazon rds with multi a-z and at least one read replica (option a)**

An it automation architecture uses many aws lambda functions invoking one another as a large state machine. The coordination of this state machine is legacy custom code that breaks easily.

Ans: **aws step functions**

4) aws account and must secure aws account root user (choose two.)

Ans: **Enable multi-factor authentication to the root user.**

Add the root user to a group containing administrative permissions.

5) you are managing an online platform which allows people to easily buy, sell , spend, and manage their cryptocurrency. To meet the strict it audit requirements, each of the api calls on all of your aws resources should be properly captured and recorded. You used cloudtrialin your vpc to help you in the compliance, operational auditing, and risk auditing of your AWS(Amazon Web Service) account.

Ans: **amazon s3**

6) a solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time

Ans: **amazon cloudfront**

7) A team of developers need to deploy a website for a development environment. The team do Manage the infrastructure and just need to upload node.js code to the instances.

Ans: **create an aws elastic beanstalk environment**

- 8) a company offers an online product brochure that is delivered from a static website running on amazon s3. The company's customers are mainly in the united states, canada, and europe. The company is looking to cost-effectively reduce the latency for users in these regions.

Ans: **Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Europe.**

- 9) a company has two accounts in an aws organization. The accounts are: prod1 and prod2.

In amazon rds database runs in the prod1 account. Amazon ec2 instances run in the prod2

Ans: **set up vpc sharing with prod1 account as the owner and the prod2 account as the participant to transfer the data**

11) An application stores transactional data in an amazon s3 bucket. The data is analyzed for the first week and then must remain immediately available for occasional analysis.

Ans: **configure a lifecycle policy to transition the objects to amazon s3 one zone-infe___ access (s3 one zone -IA) after 7 days.**

12) an it automation architecture uses many aws lambda functions invoking one another as a large state machine. The coordination of this state machine is legacy custom mode that breaks easily.

Ans: **aws step functions.**

13) a company have 500 tb of data in an on-premises file share that needs to moved to amazon s3 Glacier. The migration must not saturate the company's low-bandwidth internet connection and the migration must be completed within a few weeks. What is the most

Ans: **Order 7 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier**

which of the following distinguishes two cloudwatch metrics that are in the same namespace

Ans: **dimension**

A new application will be deployed using aws codedeploy to amazon elastic container service (ecs) . What must be supplied to codedeploy to specify the ecs service to deploy?

Ans: **the appspec file**

14) there are multiple aws accounts across multiple regions managed by a company. The operations Team require a single operational dashboard that displays some key performance metrics from these accounts and regions .

Ans: **create an amazon cloudwatch cross-account cross-region dashboard.**

17) an amazon vpc has been deployed with private and public subnets. Mysql database server running on an amazon ec2 instance will soon be launched. According to aws best practice, which subnet should the database server be launched into ?

Ans: **the private subnet**

18) your company has a set of resources hosted on the aws cloud. As a part of the new governing model, there is a requirement that all activity on aws resources should be monitored. What is the most efficient way to have this implemented?

Ans: **use aws cloudtrial to monitor all api activity.**

19) A developer needs to be notified by email for all new object creation events in a specific amazon s3 bucket. Amazon sns will be used for sending the messages. How can the developer enable these notifications?

Ans: **create an event notification for all s3:objectcreated:'API calls (option b)**

20) you have a large amount of data in amazon s3 and amazon s3 glacier that you need to move back to your on-premises datacenter. You have decided that you are going to use aws snowball to do your export. How will you export the data in amazon s3 glacier?

Ans: **Restore the data from amazon s3 glacier and then create the export request**

21) a dynamodb table is being used to store session information for users of an online game. A developer has noticed that the table size has increased considerably and much of the data is not required after a gaming session is completed.

Ans: **enable a time to live (ttl) on the table add a timestamp attribute on new (option d)**

22) A solution architect needs to select a low-cost, short-term option for adding resilience to an AWS direct connect connection. What is the most cost-effective solution to provide a backup for the direct connect connection?

Ans: **configure aws transit gateway with IPSec vpn backup.**

23) A CloudFormation template is going to be used by a global team to deploy infrastructure in several regions around the world. Which region of the template file can be used to set values based on a region?

Ans: **mappings**

24) a serverless application uses an iam role to authenticate and authorize access to an amazon dynamoDB table. A developer is troubleshooting access issues affecting the application. The developer has access to the iam role that the application is using.

Ans: **aws iam get-role-policy**

25) an application exports documents to an amazon s3 bucket. The data must be encrypted at rest and company policy mandates that encryption keys must be rotated annually. How can this be achieved automatically and with the least effort?

Ans: **use aws kms keys with automatic rotation enabled.**

26) a developer needs to add sign-up and sign-in capabilities for a mobile app. The solution should integrate with social identity providers (idps) and saml idps. Which service should the developer use? Ans: **aws cognito user pool**

27) a company recently implemented hybrid cloud connectivity using aws direct connect and is migrating data to amazon s3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and aws storage services.

Ans: **deploy an aws datasync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an aws service endpoint. (option a)**

28) an application running on amazon ec2 generates a large amount of small files (1kb each) Containing personally identifiable information that must be converted to ciphertext. The data will be stored on a proprietary network-attached file system. What is the safest way to encrypt the data using aws kms?

Ans: **Encrypt the data directly with a customer managed customer master key (Correct)**

29) you're running an rds instance that is running low on memory, resulting in slow read queries for your application . What's the most cost-effective and quickest way to resolve this?

Ans: **create a read replica.**

30) a company needs to ingest several terabytes of data every hour from a large number of distributed sources. The messages are delivered continually 24hrs a day. Messages must be delivered in real time for security analysis and live operational dashboards.

Ans: **use amazon kinesis data streams with kinesis client library to ingest and deliver messages.**

31) a company is running an ecommerce application on amazon ec2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.

Ans: **purchase reserved instances to cover 50 instances. Use on-demand and spot instances to cover the remaining instances.**

32) a static website that serves a collection of images runs an amazon s3 bucket in the us-east region. The website is gaining in popularity and is now being viewed around the world. How can a developer improve the performance of the website for global users?

Ans: **use cross region replication to the bucket to several global regions.**

33) a company uses amazon s3 as its object storage solution. The company has thousands of s3 buckets uses to store data. Some of the s3 buckets have data that is accessed less frequently than others.

Ans: **use s3 intelligent-tiering storage.**

34) a developer needs to setup a new serverless application that includes aws lambda and amazon api gateway as part of a the developer needs to be able to locally build

Ans: **aws serverless application model (sam)**

35) a development team are currently creating a new application that uses a microservices design pattern and runs on docker containers. The team would like to run the platform on aws using a managed platform. They want minimize management overhead for the platform. Which service should the development team use?

Ans: **amazon ecs with fragate launch type (option a)**

36) A company has multiple AWS accounts for several environments (prod, Dev, Test etc). A solutions architect would like to copy an amazon EBS snapshot from dev to prod. The snapshot is from an ebs volume that was encrypted with a custom key. What steps must be performed to share the encrypted ebs snapshot with the prod account?

Ans : **Modify the permissions on the encrypted snapshot to share it with the Prod account.**

Share the custom key used to encrypt the volume

38) Choose the below statements are true or false for aws

- i) when you create an iam user, you grant it permission by making it a member of a group that has.... .
- ii) you can also clone the permission of an existing iam user, which automatically makes the new user a member of.

Ans: **statement 1 and statement 2 are true**

39)A solutions architect needs a solution for hosting a website that will be used by development team. The website contents will consist of html, css, client-side javascript, and images.

Which solution is most cost-effective?

Ans: **Create an Amazon S3 bucket and host the website there.**

40) An amazon rds postgresql database is configured as multi-az. A solutions architect needs to scale read performance and the solution must be configured for high availability. What is the most cost-effective solution?

Ans: **Create a read replica as a Multi-AZ DB instance**

41) A company has deployed a new website on amazon ec2 instances behind an applicationload balancer (alb). Amazon route 53 is used for the dns service. The company has asked a solutions architect to create a backup website with support contact details that users will be directed to automatically if primary website is down. How should the solutions architect deploy this solution cost-effectively?

Ans: **Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.**

42) You have a large amount of data in Amazon s3 and Amazon s3 glacier that you need tomove back to your on-premises datacenter. You have decided that you are going to use aws snowball to do the export. How will you export the data in Amazon s3 glacier?

Ans: **Restore the data from Amazon S3 Glacier and then create the export request.**

43)Which of these is not needed for AWS Snowball setup?

Ans: **AWS Snowball client unlock code**

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

Ans **Launch a new EC2 instance from an Amazon Machine image (AMI) in a new Region**
Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination

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

Ans: **Use a target tracking policy to dynamically scale the Auto Scaling group**

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

Ans: **Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution**

47) A decoupled application is using an Amazon SQS queue. The processing layer that is retrieving messages from the queue is not able to keep up with the number of messages being placed in the queue. What is the FIRST step the developer should take to increase the number of messages the application receives?

Ans: **Use the ReceiveMessage API to retrieve up to 10 messages at a time**

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

Ans: **Create a route table entry for the endpoint**

Create a gateway endpoint for DynamoDB

48) A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website. What should a solutions architect do to meet these requirements?

Ans: **. Redesign the application to use Amazon CloudFront**

49) A company has multiple AWS accounts for several environments (prod, Dev, Test etc). A solutions architect would like to copy an Amazon EBS snapshot from dev to prod. The snapshot is from an EBS volume that was encrypted with a custom key. What steps must be performed to share the encrypted EBS snapshot with the prod account?

Ans: **Share copy**

Create a snapshots

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

Ans: **Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy**

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

Ans: **Add a deny rule in the Inbound table of the network ACL with a lower rule number than other rules.**

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

Ans: **Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0. B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.**

Configure the security group for the database tier to allow inbound traffic on port 1433 from the SecurityGroup for the web tier

53) A mobile app uploads usage information to a database. Amazon Cognito is being used for authentication, authorization and user management and users 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?

Ans: **User Pools**

54) A company has divested a single business unit and needs to move the AWS account owned by the business unit to another AWS Organization. How can this be achieved?

Ans: **Migrate the account using the AWS Organizations console**

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

Ans: **Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin**

56) A web application requires a minimum of six Amazon Elastic Compute Cloud (EC2) instances running at all times. You are tasked to deploy the application to three availability zones in the EU Ireland region (eu-west-1a, eu-west-1b, and euwest-1c). It is required that the system is fault-tolerant up to the loss of one Availability Zone. Which of the following setup is the most cost-effective solution which also maintains the fault-tolerance of your system?

Ans: **3 instances in eu-west-1a, 3 instances in eu-west-1b, and 3 instances in eu-west-1c**

57) what is the most cost-effective option for synchronous database replication with RDS?

Ans: **A multi**

58) The aws well artchitected framework does not provide.

Ans: **Architectural pattern**

59)While delivering business value through risk assessments and mitigation strategies, the security piller encompasses the ability to protect

Ans: **Information**

60)You send custom metrics to cloudwatch every 30 seconds.How should you store these metrics in cloudwatch to no matrics value are overwritten

Ans: **As high resolution metrics**

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

Ans: **Amazon CloudFront**

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

Ans: **Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.**

63) Your website has been suffering performance issues, and you have been able to determine that this is due to a spike in traffic to your servers. The servers are behind an ELB and the CPU on both Amazon EC2 instances hovers around 95% during this time frame. Your boss has asked you to find a way to improve performance without impacting cost any more than is absolutely necessary. What should you do?

Ans: Create an EC2 Auto Scaling group and have Amazon Cloud Watch trigger an autoscale event to scale up when the CPU reaches 80% and scale down when the CPU drops to 40%,

64) A Developer wants to debug an application by searching and filtering log data. The application logs are stored in Amazon CloudWatch Logs. The Developer creates a new metric filter to count exceptions in the application logs. However, no results are returned from the logs. What is the reason that no filtered results are being returned?

Ans: . CloudWatch Logs only publishes metric data for events that happen after the filter is created

65) When a developer calls the Amazon CloudWatch API, he receives HTTP 400: ThrottlingException errors sporadically. When a call is not successful, no data is obtained. Which best practice should be implemented first in order to remedy this issue?

Ans: Use the AWS CLI to get the metrics

66) A data-processing application runs on an i3.large EC2 instance with a single 100 GB EBS gp2 volume. The application stores temporary data in a small database (less than 30 GB) located on the EBS root volume. The application is struggling to process the data fast enough, and a Solutions Architect has determined that the I/O speed of the temporary database is the bottleneck. What is the MOST cost-efficient way to improve the database response times?

Ans: Move the temporary database onto instance storage.

67) A media company asked a Solutions Architect to design a highly available storage solution to serve as a centralized document store for their Amazon EC2 instances. The storage solution needs to be POSIX-compliant, scale dynamically, and be able to serve up to 100 concurrent EC2 instances.

Ans: Create an Amazon Elastic File System (Amazon EFS) to store and share the documents.

68) A Solutions Architect is designing a stateful web application that will run for one year (24/7) and then be decommissioned. Load on this platform will be constant, using a number of r4.8xlarge instances. Key drivers for this system include high availability, but elasticity is not required. What is the MOST cost-effective way to purchase compute for this platform?

Ans: Standard Reserved Instances

69) An organization developed an application that uses set of API that are served through amazon API gateway.....custom authorization model?

Ans: Use Amazon Cognito user pools and a custom authorizer to authenticate and authorize users based on JSON Web Tokens.

70) When an enterprise migrates an application to the cloud as is, without making any modifications, what is this called?

Ans: Rehost

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

Ans: Launch the EC2 instances in a cluster placement group in one Availability Zone

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

Ans: Take a snapshot of the RDS instance Create an encrypted copy of the snapshot Restore the RDS instance from the encrypted snapshot

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

Ans: Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.

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

Ans: Create a Multi-AZ RDS Read Replica of the production RDS DB instance

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

Ans: Amazon EBS

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

Ans: Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones.Store data on Amazon EFS and mount a target on each instance.

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

Ans:Enable Amazon S3 versioning

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

Ans: . Generate a presigned URL and have the vendor download the log file before it expires

79) A solution architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group..... A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

Ans: Deleting Amazon EC2 instances

80) A Solutions Architect must design a storage solution for incoming billing reports in CSV format. The data does not need to be scanned frequently and is discarded after 30 days. Which service will be MOST cost-effective in meeting these requirements?

Ans: **Write the files to an S3 bucket and use Amazon Athena to query the data.**

81) A Solutions Architect must select the most appropriate database service for two use cases. A team of data scientists perform complex queries on a data warehouse that take several hours to complete. Another team of scientists need to run fast, repeat queries and update dashboards for customer support staff. Which solution delivers these requirements MOST costeffectively?

Ans: **Redshift for both use cases.**

82) A company has deployed a new website on Amazon EC2 instances behind an Application Load Balancer (ALB). Amazon Route 53 is used for the DNS service. The company has asked a Solutions Architect to create a backup website with support contact details that users will be directed to automatically if the primary website is down. How should the Solutions Architect deploy this solution cost-effectively?

Ans: **Configure a static website using Amazon S3 and create a Route 53 failover routing policy**

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

Ans: **Configure an Amazon Route 53 geolocation routing policy**

84) A company uses an amazon s3 bucket to store a large number of sensitive files relating to ecommerce transaction. The company has policy that states that all data written to the s3 bucket must be encrypted. How can a developer ensure compliance with this policy?

Ans: **Create an S3 bucket policy that denies any S3 Put request that does not include the x-amz-server-side-encryption (Correct)**

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

Ans: **Create an Amazon EFS file system and mount it from each EC2 instance.**

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

Ans: **Configure AWS WAF on the Application Load Balancer in a VPC.**

87) Acompany runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently. Which storage service should a solutions architect use to provide the MOST cost-effective solution?

Ans: **Amazon S3**

88) ccompany hosts a static website within an Amazon \$3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion. which action will accomplish this?

Ans: **Enable Amazon S3 versioning**

89) marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the \$3 bucket. Which action will MOST securely grant the EC2 instance access to the S3 bucket?
Ans: **Associate an IAM role with least privilege permissions to the EC2 instance profile**

90) A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. SAA-C02_456q_September_2021_By_DrunkMonk The company uses tiered storage on-premises with hoi high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running. Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

Ans: **Amazon S3 for cold data storage**
Amazon FSx for clustre tor high-performance parallel storage

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

Ans: **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)**

92) A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively SAA-C02_456q_September_2021_By_DrunkMonk increases capacity to minimize any performance impact on application users. Which solution will meet these requirements?

Ans:**Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.**

93) You are responsible for deploying a critical application to AWS. It is required to ensure that the controls set for this application meet PCI compliance. Also, there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfill this requirement? Choose 2 answers from the options given below.

Ans: **Amazon CloudWatch Logs**
Amazon CloudTrail

94) Which of the following are pillars of the AWS Well-Architected Framework?

Ans: **Performance efficiency**
Security

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

Ans: **Amazon FSx**

96) A Developer has been tasked by a client to create an application. The client has provided the following requirements for the application:

- ◆ Performance efficiency of seconds with up to a minute of latency
- ◆ Data storage requirements will be up to thousands of terabytes
- ◆ Per-message sizes may vary between 100 KB and 100 MB
- ◆ Data can be stored as key/value stores supporting eventual consistency

What is the MOST cost-effective AWS service to meet these requirements?

Ans: **Amazon S3**

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

Ans: **Add Aurora Replica**

Add an Amazon CloudFront distribution in front of the Application Load Balancer

98) **Based on the following AWS CLI command the resulting output, what has happened here?**

1. \$ aws lambda invoke --function-name MyFunction --invocation-type Event --payload ewogICJrZXkxIjogInZhbHVlMSIsCiAgImtleTIIoAiAidmFsdWUyIiwKICAi a2V5MyI6ICJ2YWx1ZTMiCn0= response.json
2. {
3. "StatusCode": 202
4. }

Ans: **An AWS Lambda function has been invoked asynchronously and has completed successfully**

99)A web application is being deployed on an amazon ecs cluster using the fargate launch type. The application is expected to receive a large volume of traffic initially.The company wishes to the performance is good for the launch and that costs reduceas demand decreases.

Ans: **Use amazon ECS service Auto Scaling with target tracking policies to scale when ECS an Amazon CloudWatch alarm is breached.**

100) 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)

Ans: **Migrate the database using the AWS Database Migration Service (DMS)**

Convert the schema using the AWS Schema Conversion Tool

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

Ans: **Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy**

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

Ans: **Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked**

103) A Solutions Architect needs to design a solution that will allow Website Developers to deploy static web content without managing server infrastructure. All web content must be accessed over HTTPS with a custom domain name. The solution should be scalable as the company continues to grow.

Ans: **Amazon CloudFront with an Amazon S3 bucket origin**

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

Ans: **Use EC2 Auto Scaling lifecycle hooks to execute a custom script to send data to the audit system when instances are launched and terminated.**

105) An application deployed on AWS Elastic Beanstalk experiences increased error rates during deployments of new application versions, resulting in service degradation for users. The Development team believes that this is because of the reduction in capacity during the deployment steps. The team would like to change the deployment policy configuration of the environment to an option that maintains full capacity during deployment while using the existing instances. Which deployment policy will meet these requirements while using the existing instances?

Ans: **Rolling with additional batch**

106) A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

Ans: Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.

107) A company is investigating methods to reduce the expenses associated with on-premises backup infrastructure. The Solutions Architect wants to reduce costs by eliminating the use of physical backup tapes. It is a requirement that existing backup applications and workflows should continue to function. What should the Solutions Architect recommend?

Ans: Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL)

108) A Solutions Architect is designing an application for processing and extracting data from log files. The log files are generated by an application and the number and frequency of updates varies. The files are up to 1 GB in size and processing will take around 40 seconds for each file. Which solution is the most cost-effective?

Ans: Write the log files to an Amazon S3 bucket. Create an event notification to invoke an AWS Lambda function that will process the files

109) A company delivers content to subscribers distributed globally from an application running on AWS. The application uses a fleet of Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to an update in copyright restrictions, it is necessary to block access for specific countries. What is the EASIEST method to meet this requirement?

Ans: Use Amazon CloudFront to serve the application and deny access to blocked countries

110) A solutions architect needs to backup some application log files from an online ecommerce store to Amazon S3. It is unknown how often the logs will be accessed or which logs will be accessed the most. The solutions architect must keep costs as low as possible by using the appropriate S3 storage class. Which S3 storage class should be implemented to meet these requirements?

Ans: S3 Intelligent Tiering

111) A Developer created a new AWS account and must create a scalable AWS Lambda function that meets the following requirements for concurrent execution: ➔ Average execution time of 100 seconds ➔ 50 requests per second Which step must be taken prior to deployment to prevent errors?

Ans: Contact AWS Support to increase the concurrent execution limits

112) You update a custom CloudWatch metric with the timestamp of 15:57:08 and a value of 3. You then update the same metric with the timestamp of 15:57:37 and a value of 6. Assuming the metric is a high-resolution metric, which of the following will CloudWatch do?

Ans: Record both values with the given timestamp.

113) A development team manage a high-traffic e-Commerce site with dynamic pricing that is updated in real-time. There have been incidents where multiple updates occur simultaneously and cause an original editor's updates to be overwritten. How can the developers ensure that overwriting does not occur?

Ans: Use conditional writes

114) an aws lambda function has been connected to a vpc to access an application running a private subnet. The lambda function also pulls data from an internet based service and is no longer able to connect to the interenet how can this be rectified

Ans: Add a NAT Gateway to public subnet and specify

115)A development team is involved with migrating an on-premises MySQL database to amazon RDS. The database usage is very read-heavy. The development team wants to re-factor the application code to achieve optimum read performance for queries.

How can this objective be met?

Ans: Add a connection string to use an RDS read replica for read queries

116) an organization has an account for each environment. Production, testing, development. A developer with an IAM user in the development account....

Ans: Create an IAM group in the production and testing account and add the developer from the development account to the groups.

117) A retail organization sends coupons out twice a week and this results in a predictable surge in sales traffic. The application runs on Amazon EC2 instances behind an Elastic Load Balancer. The organization is looking for ways to reduce cost without impacting performance or reliability. How can they achieve this goal?

Ans: Purchase scheduled reserved instances

118) **A company is using AWS Lambda for processing small images that are uploaded to Amazon S3. This was working well until a large number of small files (several thousand) were recently uploaded and an error was generated by AWS Lambda (status code 429).**

Ans: The concurrency execution limit for the account has been exceeded

119) **An application requires an in-memory caching engine. The cache should provide high availability as repopulating data is expensive. How can this requirement be met?**

Ans: Use Amazon ElastiCache Redis with replicas

120) **An application is being migrated into the cloud. The application is stateless and will run on a fleet of Amazon EC2 instances. The application should scale elastically. How can a Developer ensure that the number of instances available is sufficient for current demand?**

Ans: Create a launch configuration and use Amazon EC2 Auto Scaling

SAA-C02_456q_September _2021_By_DrunkMonk

Passing Score: 800

Time Limit: 120 min

File Version: 1.0

Vendor: Amazon

Exam Code: SAA-C02

Exam Name: AWS Certified Solutions Architect - Associate

(SAA-C02) Exam

Exam A

QUESTION 1

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second.

The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth Data can be queried using simple key-value requests. Which combination of AWS services would meet these requirements? (Select TWO)

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In this case AWS Lambda can perform the computation and store the data in an Amazon DynamoDB table. Lambda can scale concurrent executions to meet demand easily and DynamoDB is built for key-value data storage requirements and is also serverless and easily scalable. This is therefore a cost effective solution for unpredictable workloads.

CORRECT: "AWS Lambda" is a correct answer.

CORRECT: "Amazon DynamoDB" is also a correct answer.

INCORRECT: "AWS Fargate" is incorrect as containers run constantly and therefore incur costs even when no requests are being made.

INCORRECT: "Amazon EC2 Auto Scaling" is incorrect as this uses EC2 instances which will incur costs even when no requests are being made.

INCORRECT: "Amazon RDS" is incorrect as this is a relational database not a No-SQL database. It is therefore not suitable for key-value data storage requirements.

References:

<https://aws.amazon.com/lambda/features/>

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

QUESTION 2

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning.

This application runs on AWS Fargate and the connected storage needs to have concurrent access to files and deliver high performance.

Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Keyword: Concurrent Access to files + Deliver High Performance Amazon FSx -

A high-performance file system optimized for fast processing of workloads. Lustre is a popular open-source parallel file system.

Also supports concurrent access to the same file or directory from thousands of compute instances.

Amazon IAM with FSx -

take to manage your file systems (such as creating and deleting file systems).

groups can take based on those tags.

Fargate Launch Type - So, Answer C & D Ruled-out as per Neal David Fargate automatically provisions resources



Fargate provisions and manages compute



Charged for running tasks



No EFS and EBS integration



Fargate handles cluster optimization



Limited control, infrastructure is automated

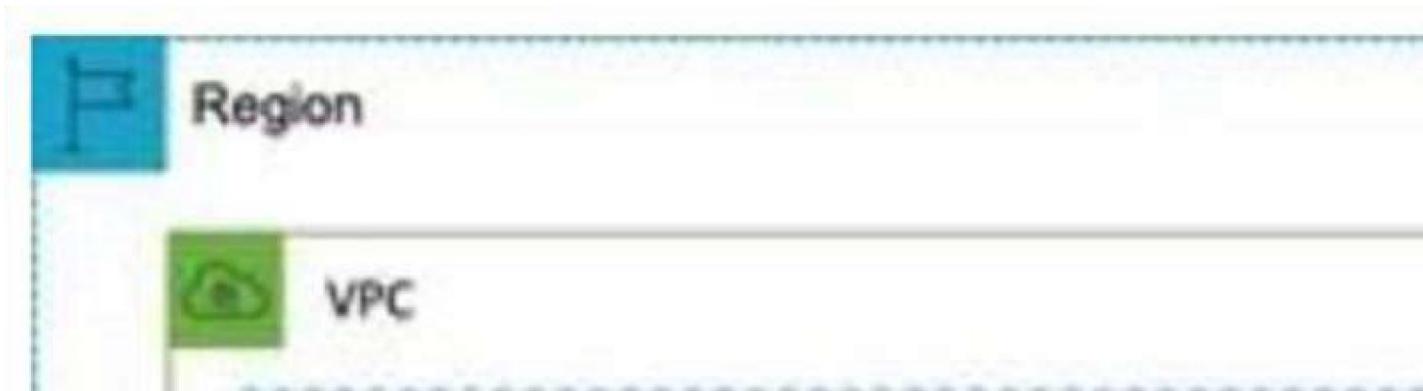


QUESTION 3

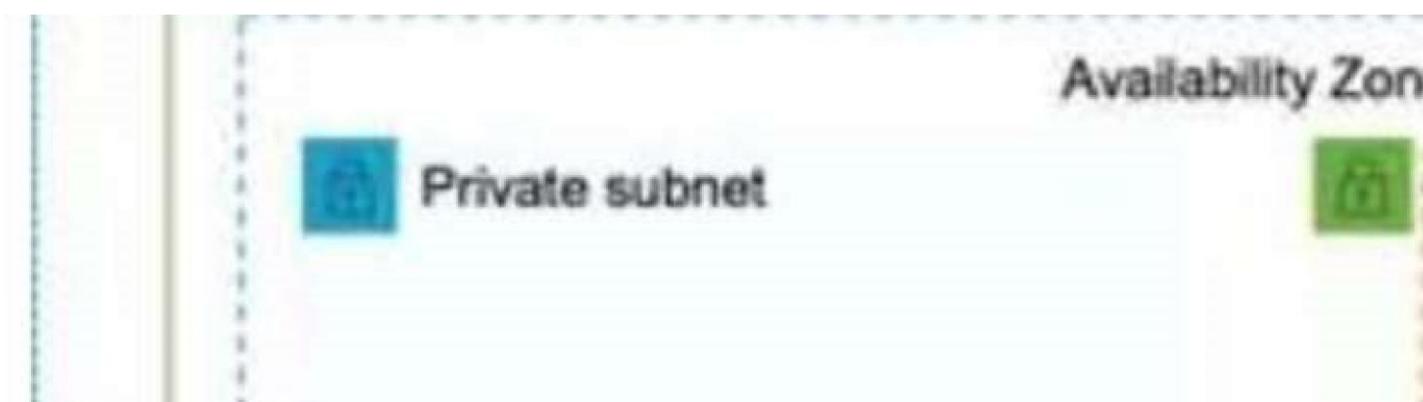
A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application. Which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

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

Correct Answer: B



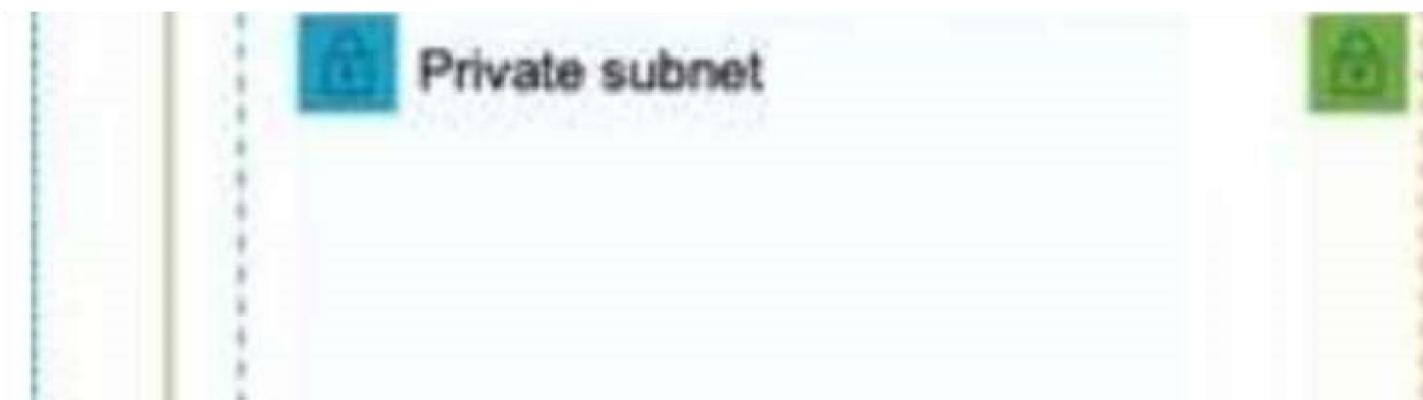
Section: (none)



Explanation

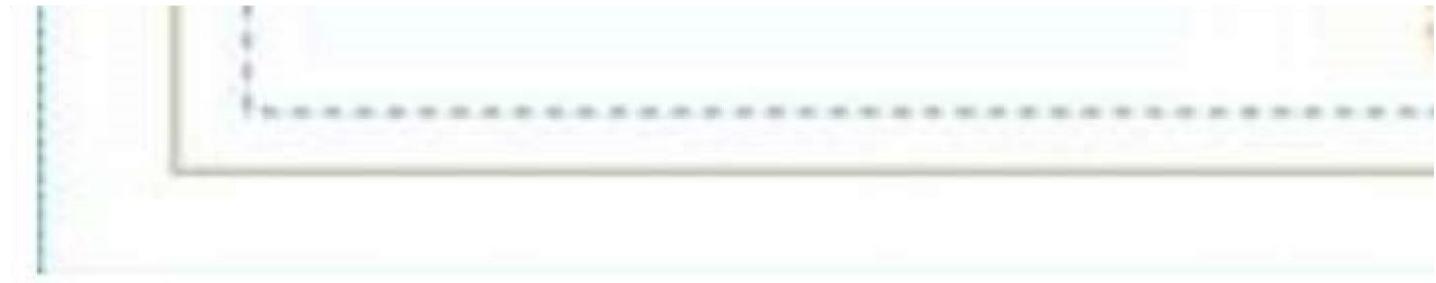


Explanation/Reference:



Explanation:

High availability can be enabled for this architecture quite simply by modifying the existing Auto Scaling group to use multiple availability zones. The ASG will automatically balance the load so as per AZ. The architecture for the web tier will look like the one below:



CORRECT: "Modify the Auto Scaling group to use four instances across each of two Availability Zones" is the correct answer.

INCORRECT: "Create an Auto Scaling group that uses four instances across each of two Regions" is incorrect as EC2 Auto Scaling does not support multiple regions. INCORRECT: "Create an Auto Scaling template that can be used to quickly create more instances in another Region" is incorrect as EC2 Auto Scaling does not support multiple regions. INCORRECT: "Create an Auto Scaling group that uses four instances across each of two subnets" is incorrect as the subnets could be in the same AZ.

References:

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

QUESTION 4

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer.

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Though this sounds like a good use case for scheduled actions, both answers using scheduled actions will have 20 instances running regardless of actual demand. A better option to be more cost effective is to use a target tracking action that triggers at a lower CPU threshold.

Auto Scaling Group

With this solution the scaling will occur before the CPU utilization gets to a point where performance is

affected. This will result in resolving the performance issues whilst minimizing costs. Using a reduced

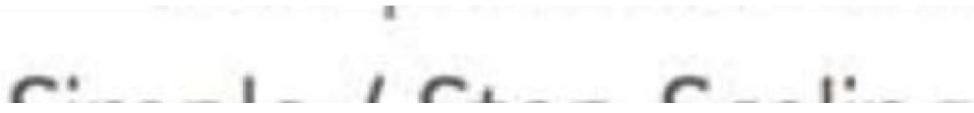
• Target Tracking Scaling

cooldown period will also more quickly terminate unneeded instances, further reducing costs.



- Most simple and easy to set

- Example: I want the average



• Simple / Step Scaling

- When a CloudWatch alarm



- When a CloudWatch alarm

• Scheduled Actions



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

- Anticipate a scaling based on

tracking.html

- Example: increase the min c

QUESTION 5

QUESTION 5

A solutions architect is designing a solution to access a catalog of images and provide users with the ability

to submit requests to customize images.

Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image.

The solution must be highly available for viewing and customizing images. What is the MOST cost-effective solution to meet these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

All solutions presented are highly available. The key requirement that must be satisfied is that the solution should be cost-effective and you must choose the most cost-effective option.

Lambda, Amazon S3 and CloudFront are the best services to use for these requirements. CORRECT:

"Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is the correct answer. INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3.

Configure an Elastic Load Balancer in front of the EC2 instances" is incorrect. This is not the most cost-effective option as the ELB and EC2 instances will incur costs even when not used. INCORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon

"EC2 instances" is incorrect. This is not the most cost-effective option as the ELB will incur costs even when not used. Also, Amazon DynamoDB will incur RCU/WCUs when running and is not the best choice for storing images.

INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is incorrect. This is not the most cost-effective option as the EC2 instances will incur costs even when not used References: <https://aws.amazon.com/serverless/>

QUESTION 6

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours.

The company wants to use these data points in its existing analytics platform A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API. Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3
- B. Use Amazon API Gateway with AWS Lambda
- C. Use Amazon QuickSight with Amazon Redshift
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Keyword: Data points in its existing analytics platform + Data points must be accessible from the REST API + Track the location of its bicycles during peak operating hours

They already have an analytics platform, A (Athena) and D (Kinesis Data Analytics) are out of the race even though S3 & API Gateway Support REST API. Now B and C are in Race. C will not support REST API. So answer should be B as per below details.

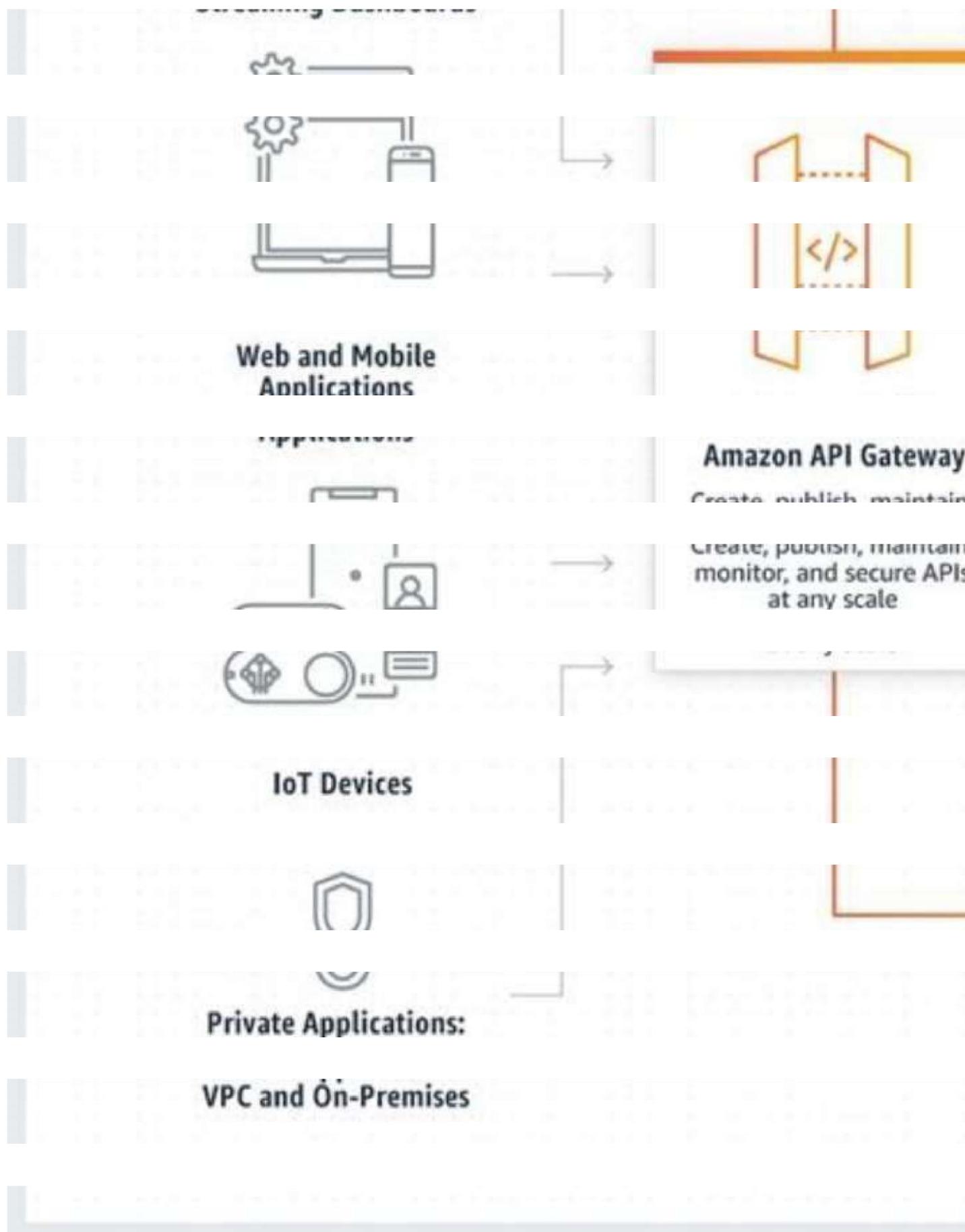
Now if we talk about data type, we are talking about GEO location data for their bicycles. API Gateway will

be support REST API. So, exact solution should be API Gateway with AWS Lambda along with Amazon

Kinesis Data Analytics (Assume its used already).



**Connected Users and
Streaming Dashboards**



CORRECT: "Use Amazon API Gateway with AWS Lambda" is the correct answer. INCORRECT: "Use Amazon Athena with Amazon S3" is incorrect as they already have analytics platform.
INCORRECT: "Use Amazon QuickSight with Amazon Redshift" is incorrect. This is not support REST API.
INCORRECT: "Use Amazon API Gateway with Amazon Kinesis Data Analytics" is incorrect as they already have analytics platform.

References: <https://aws.amazon.com/api-gateway/> <https://aws.amazon.com/lambda/> <https://aws.amazon.com/kinesis/data-analytics/>

QUESTION 7

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

- A. Amazon EBS
- B. Amazon EC2 instance store
- C. Amazon EFS
- D. Amazon S3

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

It is block storage made for high throughput and low latency. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

QUESTION 8

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet.

What should the solutions architect do to accomplish this? (Select TWO)

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

Correct Answer: AB

Section: (none)

Explanation

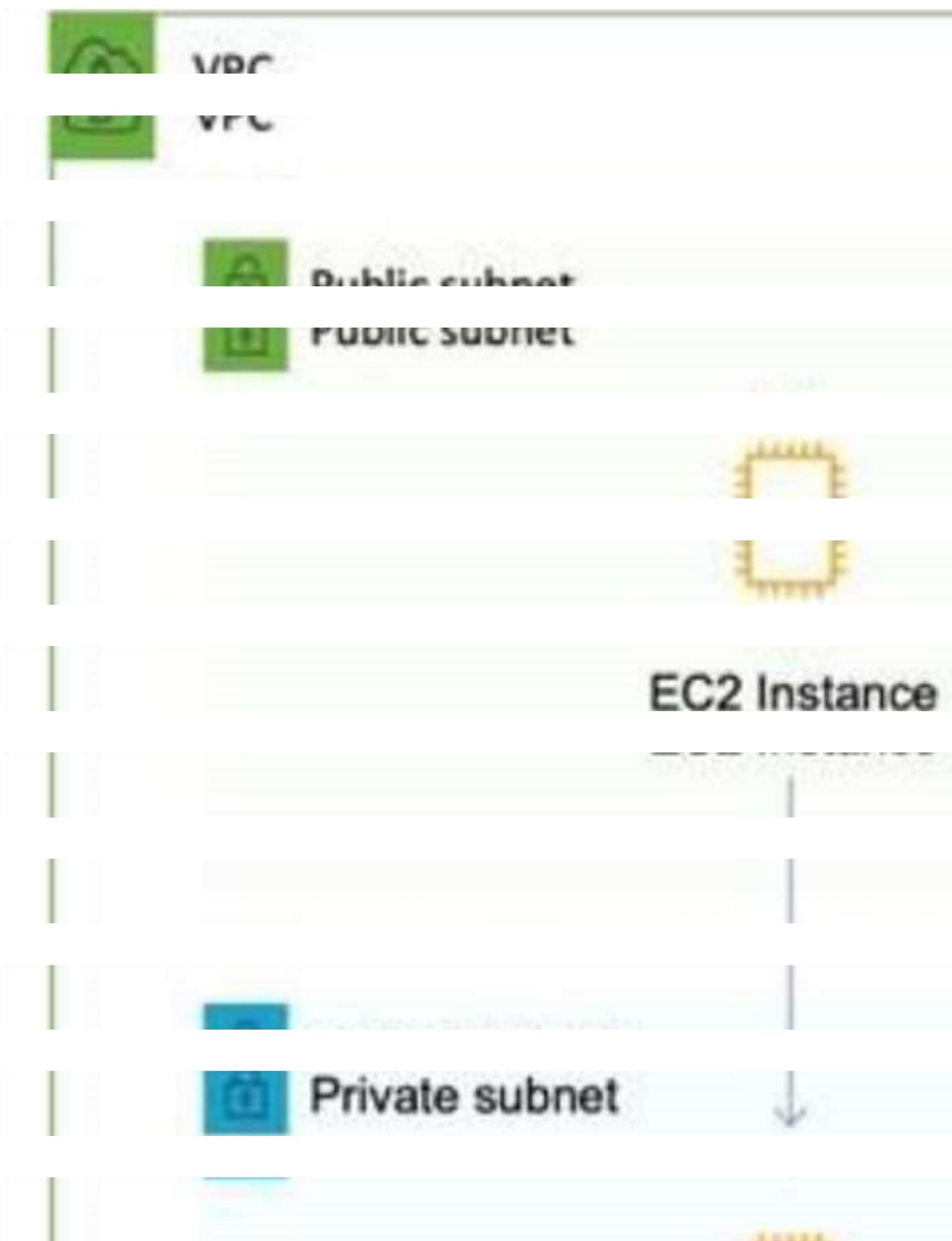
Explanation/Reference:

Explanation:

Amazon DynamoDB and Amazon S3 support gateway endpoints, not interface endpoints. With a gateway endpoint you create the endpoint in the VPC, attach a policy allowing access to the service, and then

Default VPC

specify the route table to create a route table entry in.





EC2 Instance

Route Table

Destinat

pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.2

CORRECT: "Create a route table entry for the endpoint" is a correct answer. CORRECT: "Create a

gateway endpoint for DynamoDB" is also a correct answer. INCORRECT: "Create a new DynamoDB table that uses the endpoint" is incorrect as it is not necessary to create a new DynamoDB table.

INCORRECT: "Create an ENI for the endpoint in each of the subnets of the VPC" is incorrect as an ENI is used by an interface endpoint, not a gateway endpoint. INCORRECT: "Create a VPC peering connection between the VPC and DynamoDB" is incorrect as you cannot create a VPC peering connection between a VPC and a public AWS service as public services are outside of VPCs.

References: <https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html>

QUESTION 9

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB).

The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.

What should the solutions architect recommend?

- A. Leverage Amazon CloudFront with the ALB endpoint as the origin
- B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB
- C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked
- D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances

instances

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://aws.amazon.com/waf/>

<https://aws.amazon.com/shield/>

<https://aws.amazon.com/shield/features/>

QUESTION 10

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

Which solution should the solutions architect suggest?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This question is simply asking you to work out the best compute service for the stated requirements. The key requirements are that the compute service should be suitable for a workload that can range quite broadly in demand from no requests to large bursts of traffic. AWS Lambda is an ideal solution as you pay

only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.

CORRECT: "Set up an Amazon API Gateway and use AWS Lambda functions" is the correct answer.

INCORRECT: "Set up an Amazon API Gateway and use Amazon ECS" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic. INCORRECT: "Set up an Amazon API Gateway and use AWS Elastic Beanstalk" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic. INCORRECT: "Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic. References: <https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html>

QUESTION 11

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes.

The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID).

What should a solutions architect do to meet these requirements?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To increase the resiliency of the application the solutions architect can use Auto Scaling groups to launch and terminate instances across multiple availability zones based on demand. An application load balancer (ALB) can be used to direct traffic to the web application running on the EC2 instances.

Lastly, the Amazon Elastic File System (EFS) can assist with increasing the resilience of the application by providing a shared file system that can be mounted by multiple EC2 instances from multiple availability zones.

CORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance" is the correct answer.

INCORRECT: "Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance" is incorrect as the EBS volumes are single points of failure which are not shared with other instances.

INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance" is incorrect as instance stores are ephemeral data stores which means data is lost when powered down. Also, instance stores cannot be shared between instances.

INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as there are data retrieval charges associated with this S3 tier. It is not a suitable storage tier for application files. References: <https://docs.aws.amazon.com/efs/>

QUESTION 12

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

- A. Store the password in AWS CloudHSM.
Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.
- B. Store the password in AWS Secrets Manager.
Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.
- C. Move the database password to an environment variable associated with the Lambda function. Retrieve the password from the environment variable upon execution.
- D. Store the password in AWS Key Management Service (AWS KMS).
Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

A solutions architect needs the static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.

Which action will accomplish this?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Object versioning is a means of keeping multiple variants of an object in the same Amazon S3 bucket. Versioning provides the ability to recover from both unintended user actions and application failures. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket.

CORRECT: "Enable Amazon S3 versioning" is the correct answer. **INCORRECT:** "Enable Amazon S3 Intelligent-Tiering" is incorrect. This is a storage class that automatically moves data between frequent access and infrequent access classes based on usage patterns.

INCORRECT: "Enable an Amazon S3 lifecycle policy" is incorrect. An S3 lifecycle policy is a set of rules that define actions that apply to groups of S3 objects such as transitioning objects to another storage class.

INCORRECT: "Enable Amazon S3 cross-Region replication" is incorrect as this is used to copy objects to different regions. CRR relies on versioning which is the feature that is required for protecting against accidental deletion.

References: <https://d0.awsstatic.com/whitepapers/protecting-s3-against-object-deletion.pdf>

QUESTION 14

A company is managing health records on-premises.

The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is

running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records.

Which services can the solutions architect recommend to meet these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Keyword: Move existing data and support future records + Granular audit access at all levels

Use AWS DataSync to migrate existing data to Amazon S3, and then use the File Gateway configuration of AWS Storage Gateway to retain access to the migrated data and for ongoing updates from your on-premises file-based applications.

Need a solution to move existing data and support future records = AWS DataSync should be used for migration.

Need granular audit access at all levels = Data Events should be used in CloudTrail, Management Events is enabled by default.

CORRECT: "Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new



data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events" is the correct answer.

INCORRECT: "Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events" is incorrect as "current infrastructure is running out of space" INCORRECT: "Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events." is incorrect as "Management Events is enabled by default" INCORRECT: "Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic

Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging." is incorrect as "current infrastructure is running out of space"



How AWS DataSync Works



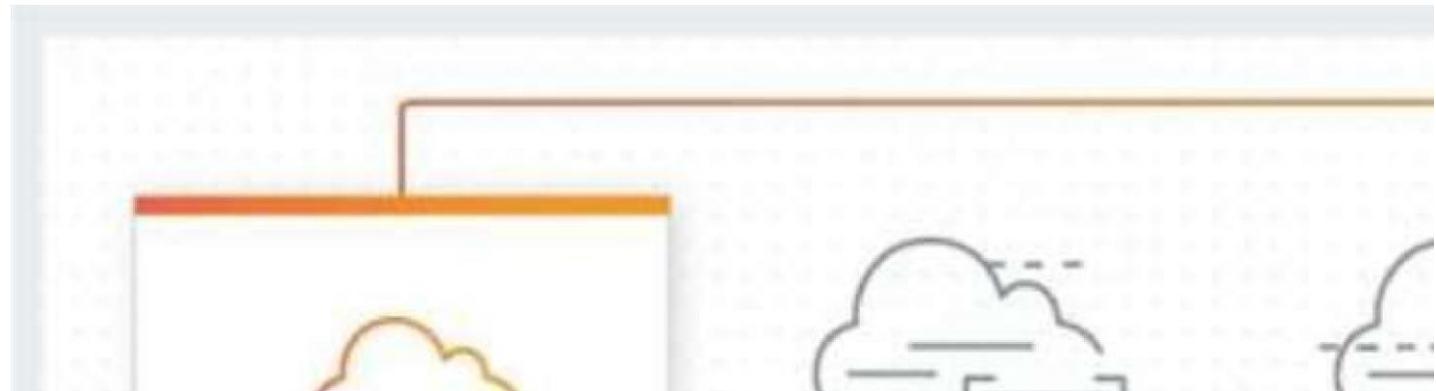
AWS DataSync Agent

The DataSync agent is deployed as a VM and

connects to your NAS or file system to copy data to AWS and write data from AWS

How AWS CloudTrail works References:

[https://aws.amazon.com/datasync/?whats-new-cards.sort-](https://aws.amazon.com/datasync/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whatsnew-cards.sort-order=desc)



[by=item.additionalFields.postDateTime&whatsnew-cards.sort-order=desc](https://aws.amazon.com/datasync/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whatsnew-cards.sort-order=desc)

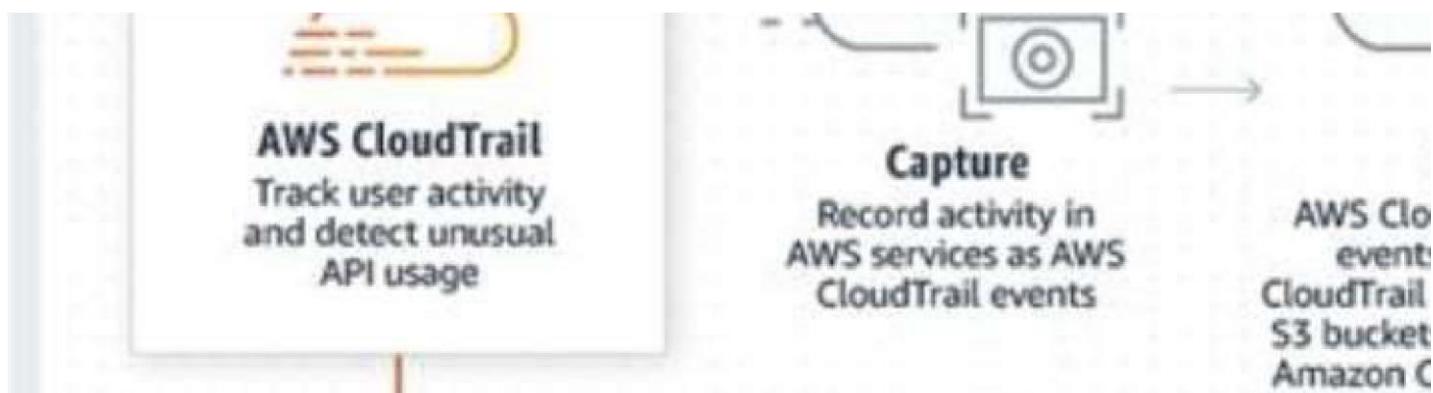
<https://aws.amazon.com/cloudtrail/> <https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

QUESTION 15

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed.

The company will make at least one encrypted backup before destroying the old backups. What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored



- B. Modify the backup section of the database configuration to toggle the Enable encryption check box.

- C. Create a snapshot of the database.
Copy it to an encrypted snapshot.
Restore the database from the encrypted snapshot.
- D. Enable an encrypted read replica on RDS for MySQL.
Promote the encrypted read replica to primary.
Remove the original database instance.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon RDS uses snapshots for backup. Snapshots are encrypted when created only if the database is encrypted and you can only select encryption for the database when you first create it. In this case the database, and hence the snapshots, are unencrypted. However, you can create an encrypted copy of a snapshot. You can restore using that snapshot which creates a new DB instance that has encryption enabled. From that point on encryption will be enabled for all snapshots.

CORRECT: "Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot" is the correct answer. **INCORRECT:** "Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance" is incorrect as you cannot create an encrypted read replica from an unencrypted master.

INCORRECT: "Modify the backup section of the database configuration to toggle the Enable encryption check box" is incorrect as you cannot add encryption for an existing database. **INCORRECT:** "Enable default encryption for the Amazon S3 bucket where backups are stored" is incorrect because you do not have access to the S3 bucket in which snapshots are stored. References:

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

QUESTION 16 A client reports that they want see an audit log of any changes made to AWS resources in their account.

What can the client do to achieve this?

- A. Set up Amazon CloudWatch monitors on services they own
- B. Enable AWS CloudTrail logs to be delivered to an Amazon S3 bucket
- C. Use Amazon CloudWatch Events to parse logs
- D. Use AWS OpsWorks to manage their resources

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A CloudTrail trail can be created which delivers log files to an Amazon S3 bucket.

QUESTION 17

An application running in a private subnet accesses an Amazon DynamoDB table. There is a security requirement that the data never leave the AWS network.

How should this requirement be met?

- A. Configure a network ACL on DynamoDB to limit traffic to the private subnet
- B. Enable DynamoDB encryption at rest using an AWS KMS key
- C. Add a NAT gateway and configure the route table on the private subnet
- D. Create a VPC endpoint for DynamoDB and configure the endpoint policy

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Hint: Private Subnet = VPC Endpoint

QUESTION 18

A three-tier application is being created to host small news articles. The application is expected to serve millions of users. When breaking news occurs, the site must handle very large spikes in traffic without significantly impacting database performance.



What **Elastic Network Interface**

Definition

Private IP

Which design meets these requirements while minimizing costs?

How

Uses DNS entries to red

- A. Use Auto Scaling groups to increase the number of Amazon EC2 instances delivering the

webapplication

- B. Use Auto Scaling groups to increase the size of the Amazon RDS instances delivering the database

- C. Use Amazon DynamoDB strongly consistent reads to adjust for the increase in traffic

- D. Use Amazon DynamoDB Accelerator (DAX) to cache read operations to the database

Correct Answer: D

Security Security Groups

Section: (none)

Explanation

Explanation/Reference:

Explanation:

DAX has in memory cache. If breaking news happens, majority of the users searching will look for the exact same thing. That being said, requests will query the Memory Cache first and will not need to fetch the data from the DB directly.

QUESTION 19

During a review of business applications, a Solutions Architect identifies a critical application with a relational database that was built by a business user and is running on the user's desktop. To reduce the risk of a business interruption, the Solutions Architect wants to migrate the application to a highly available, multi-tiered solution in AWS.

What should the Solutions Architect do to accomplish this with the LEAST amount of disruption to the business?

- A. Create an import package of the application code for upload to AWS Lambda, and include a function to create another Lambda function to migrate data into an Amazon RDS database
- B. Create an image of the user's desktop, migrate it to Amazon EC2 using VM Import, and place the EC2 instance in an Auto Scaling group
- C. Pre-stage new Amazon EC2 instances running the application code on AWS behind an Application Load Balancer and an Amazon RDS Multi-AZ DB instance
- D. Use AWS DMS to migrate the backend database to an Amazon RDS Multi-AZ DB instance. Migrate the application code to AWS Elastic Beanstalk

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

A company has thousands of files stored in an Amazon S3 bucket that has a well-defined access pattern. The files are accessed by an application multiple times a day for the first 30 days. Files are rarely accessed within the next 90 days. After that, the files are never accessed again. During the first 120 days, accessing these files should never take more than a few seconds.

Which lifecycle policy should be used for the S3 objects to minimize costs based on the access pattern?

- A. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage for the first 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.
- B. Use Amazon S3 Standard storage for the first 30 days. Then move the files to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the next 90 days. Allow the data to expire after that.
- C. Use Amazon S3 Standard storage for first 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.
- D. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the first 30 days. After that, move the data to the GLACIER storage class, where it will be deleted automatically.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

It is mentioned that they need to access data in few seconds during the 120 days.

QUESTION 21

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week. CORRECT: "Scheduled Reserved Instances" is the correct answer. INCORRECT: "Standard Reserved Instances" is incorrect as the workload only runs for 4 hours a day this would be more expensive.

INCORRECT: "On-Demand Instances" is incorrect as this would be much more expensive as there is no discount applied.

INCORRECT: "Spot Instances" is incorrect as the workload cannot be interrupted once started. With Spot instances workloads can be terminated if the Spot price changes or capacity is required.

References: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

QUESTION 22

An application generates audit logs of operational activities. Compliance requirements mandate that the application retain the logs for 5 years. How can these requirements be met?

- A. Save the logs in an Amazon S3 bucket and enable Multi-Factor Authentication Delete (MFA Delete) on the bucket.
- B. Save the logs in an Amazon EFS volume and use Network File System version 4 (NFSv4) locking with the volume.
- C. Save the logs in an Amazon Glacier vault and use the Vault Lock feature.
- D. Save the logs in an Amazon EBS volume and take monthly snapshots.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon Glacier, which enables long-term storage of mission-critical data, has added Vault Lock. This new feature allows you to lock your vault with a variety of compliance controls that are designed to support such long-term records retention.

QUESTION 23

A Solutions Architect is creating an application running in an Amazon VPC that needs to access AWS Systems Manager Parameter Store. Network security rules prohibit any route table entry with a 0.0.0.0/0 destination.

What infrastructure addition will allow access to the AWS service while meeting the requirements?

- A. VPC peering
- B. NAT instance
- C. NAT gateway
- D. AWS PrivateLink

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To publish messages to Amazon SNS topics from an Amazon VPC, create an interface VPC endpoint.

Then, you can publish messages to SNS topics while keeping the traffic within the network that you manage with the VPC. This is the most secure option as traffic does not need to traverse the Internet.

CORRECT: "Use AWS PrivateLink" is the correct answer. INCORRECT: "Use an Internet Gateway" is incorrect. Internet Gateways are used by instances in public subnets to access the Internet and this is less

secure than an VPC endpoint. INCORRECT: "Use a proxy instance" is incorrect. A proxy instance will also use the public Internet and so is less secure than a VPC endpoint.

INCORRECT: "Use a NAT gateway" is incorrect. A NAT Gateway is used by instances in private subnets to access the Internet and this is less secure than an VPC endpoint.

References: <https://docs.aws.amazon.com/sns/latest/dg/sns-vpc-endpoint.html>

QUESTION 24

A photo-sharing website running on AWS allows users to generate thumbnail images of photos stored in Amazon S3. An Amazon DynamoDB table maintains the locations of photos, and thumbnails are easily recreated from the originals if they are accidentally deleted.

How should the thumbnail images be stored to ensure the LOWEST cost?

- A. Amazon S3 Standard-Infrequent Access (S3 Standard-IA) with cross-region replication
- B. Amazon S3
- C. Amazon Glacier
- D. Amazon S3 with cross-region replication

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

A company is implementing a data lake solution on Amazon S3. Its security policy mandates that the data stored in Amazon S3 should be encrypted at rest.

Which options can achieve this? (Select TWO.)

- A. Use S3 server-side encryption with an Amazon EC2 key pair.
- B. Use S3 server-side encryption with customer-provided keys (SSE-C).
- C. Use S3 bucket policies to restrict access to the data at rest.
- D. Use client-side encryption before ingesting the data to Amazon S3 using encryption keys.
- E. Use SSL to encrypt the data while in transit to Amazon S3.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Enable MFA"

The AWS Account Root User - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

"Choose a strong password"

Changing the AWS Account Root User Password -

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_change-root.html

QUESTION 27

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight the application becomes much slower when the month-end financial calculation batch executes.

This causes the CPU utilization of the EC2 instances to immediately peak to 100% which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Scheduled scaling allows you to set your own scaling schedule. In this case the scaling action can be scheduled to occur just prior to the time that the reports will be run each month. Scaling actions are performed automatically as a function of time and date. This will ensure that there are enough EC2 instances to serve the demand and prevent the application from slowing down. CORRECT: "Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule" is the correct answer.

INCORRECT: "Configure an Amazon CloudFront distribution in front of the ALB" is incorrect as this would be more suitable for providing access to global users by caching content. INCORRECT: "Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization" is incorrect as this would not prevent the slowdown from occurring as there would be a delay between when the CPU hits 100% and the metric being reported and additional instances being launched.

INCORRECT: "Configure Amazon ElastiCache to remove some of the workload from the EC2 instances" is incorrect as ElastiCache is a database cache, it cannot replace the compute functions of an EC2 instance.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

QUESTION 28

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

A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

- A. Amazon EFS
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Correct Answer: B

Section: (none)**Explanation****Explanation/Reference:**

Explanation:

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs). Additionally, Amazon FSx for Windows File Server supports Distributed File System Replication (DFSR) in both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.

CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems. INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.

INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.

References: <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-single.html>

Deployment type	SSD storage	HDD storage
Single-AZ 1		
Single-AZ 2	✓	✓
Multi-AZ	✓	✓

QUESTION 29

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB).

There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks.

The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website. What should a solutions architect do to protect the application?

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

- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A new version of the AWS Web Application Firewall was released in November 2019. With AWS WAF classic you create "IP match conditions", whereas with AWS WAF (new version) you create "IP set match statements". Look out for wording on the exam. The IP match condition / IP set match statement inspects the IP address of a web request's origin against a set of IP addresses and address ranges. Use this to allow or block web requests based on the IP addresses that the requests originate from. AWS WAF supports all IPv4 and IPv6 address ranges. An IP set can hold up to 10,000 IP addresses or IP address ranges to check.

CORRECT: "Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address" is the correct answer.

INCORRECT: "Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address" is incorrect as CloudFront does not sit within a subnet so network ACLs do not apply to it.

INCORRECT: "Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address" is incorrect as the source IP addresses of the data in the EC2 instances' subnets will be the ELB IP addresses.

INCORRECT: "Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address." is incorrect as you cannot create deny rules with security groups.

References: <https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html>

QUESTION 30

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Keyword: Privilege Permission + IAM Role

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

IAM is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS services by your users.

IAM roles for Amazon EC2

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other

users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows: Create an IAM role.

■

Define which accounts or AWS services can assume the role.

■

Define which API actions and resources the application can use after assuming the role.

■

Specify the role when you launch your instance, or attach the role to an existing instance.

■

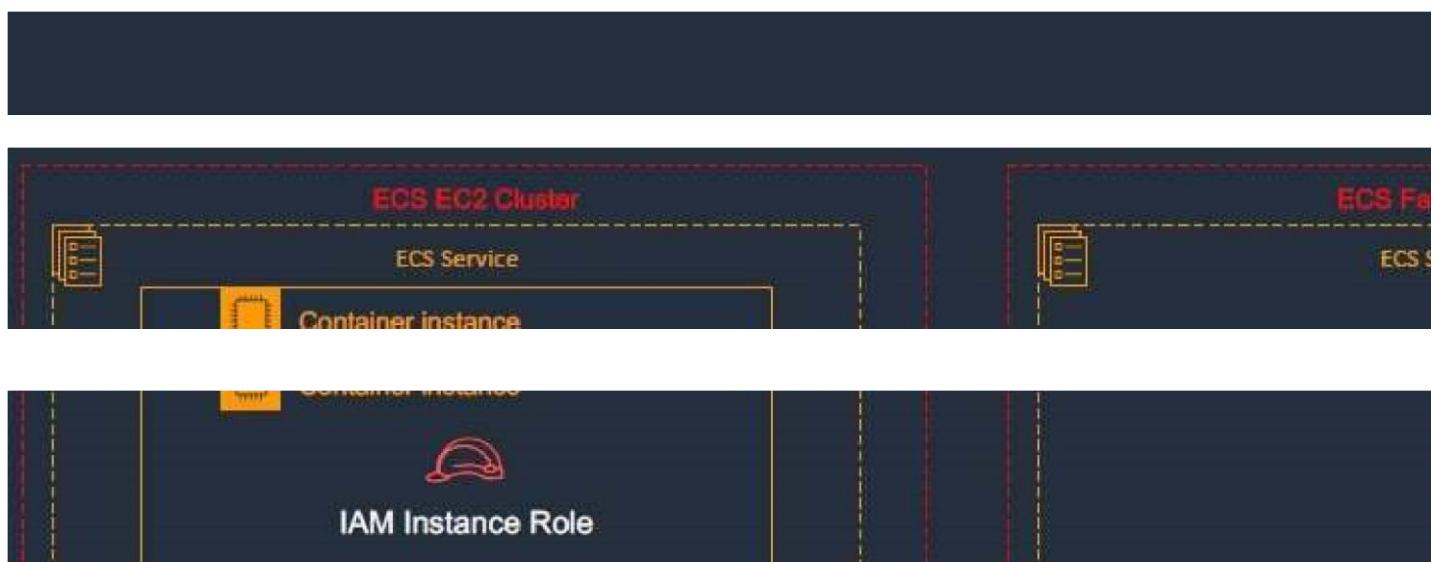
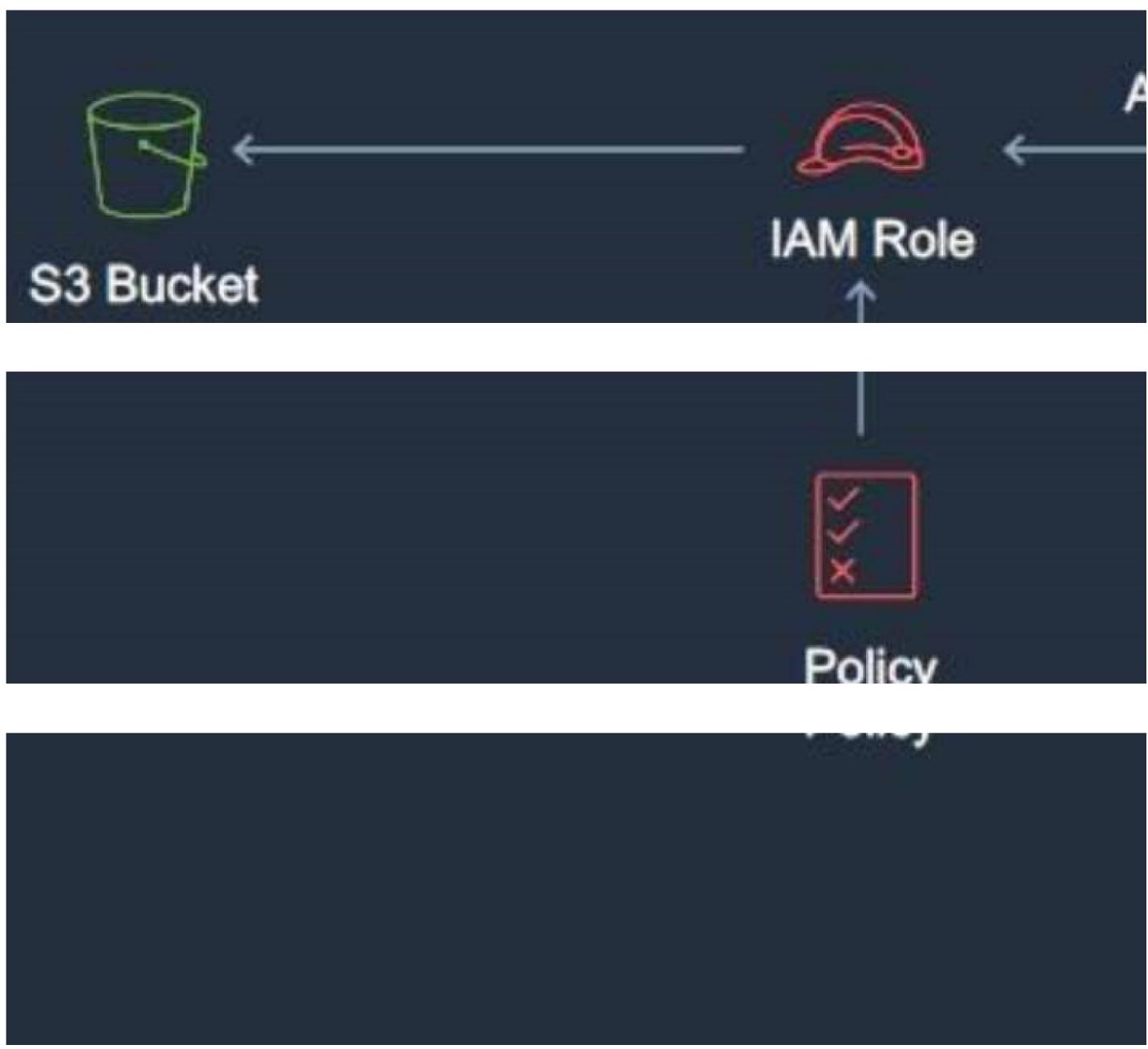
Have the application retrieve a set of temporary credentials and use them.

■

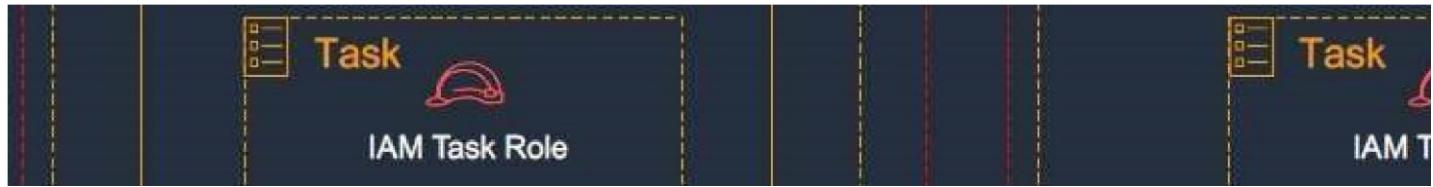
For example, you can use IAM roles to grant permissions to applications running on your instances that need to use a bucket in Amazon S3. You can specify permissions for IAM roles by creating a policy in JSON format. These are similar to the policies that you create for IAM users. If you change a role, the change is propagated to all instances.

When creating IAM roles, associate least privilege IAM policies that restrict access to the specific API calls the application requires.

IAM Roles



References:



<https://aws.amazon.com/iam/faqs/>



<https://youtu.be/YQsK4MtsELU>

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

QUESTION 31

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable.

The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).

Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Using Amazon CloudFront as the front-end provides the option to specify a custom message instead of the default message. To specify the specific file that you want to return and the errors for which the file should be returned, you update your CloudFront distribution to specify those values. For example, the following is a customized error message:



Web services

Java Platform, Enterprise Edition

Java Platform, Standard Edition



The CloudFront distribution can use the ALB as the origin, which will cause the website content to be

cached on the CloudFront edge caches.

This solution represents the most operationally efficient choice as no action is required in the event of an

issue, other than troubleshooting the root cause.

References: <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/custom-error-pages.html>

QUESTION 32

A solutions architect is designing the cloud architecture for a new application being deployed on AWS.

The process should run in parallel while adding and removing application nodes as needed based on

the number of jobs to be processed. The processor application is stateless.

The solutions architect must ensure that the application is loosely coupled and the job items are durably

stored.

Which design should the solutions architect use?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In this case we need to find a durable and loosely coupled solution for storing jobs. Amazon SQS is ideal for this use case and can be configured to use dynamic scaling based on the number of jobs waiting in the queue.

To configure this scaling you can use the backlog per instance metric with the target value being the acceptable backlog per instance to maintain. You can calculate these numbers as follows:

Backlog per instance: To calculate your backlog per instance, start with the

ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.

Acceptable backlog per instance: To calculate your target value, first determine what your application can accept in terms of latency. Then, take the acceptable latency value and divide it by the average time that an EC2 instance takes to process a message. This solution will scale EC2 instances using Auto Scaling based on the number of jobs waiting in the SQS queue.

CORRECT: "Create an Amazon SQS queue to hold the jobs that needs to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue" is the correct answer.

INCORRECT: "Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage" is incorrect as scaling on network usage does not relate to the number of jobs waiting to be processed. **INCORRECT:** "Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages

Auto Scaling group to add and remove nodes based on CPU usage" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on CPU usage is not the best solution as it does not relate to the number of jobs waiting to be processed. **INCORRECT:** "Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages

published to the SNS topic" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on the number of notifications in SNS is not possible.

References: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

QUESTION 33

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This is a good use case for Amazon SQS. The microservices must be decoupled so they can scale independently. An Amazon SQS queue will enable microservice 1 to add messages to the queue.

Microservice 2 can then pick up the messages and process them. This ensures that if there's a spike in traffic on the frontend, messages do not get lost due to the backend process not being ready to process them.

CORRECT: "Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue" is the correct answer. INCORRECT: "Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2" is incorrect as a message queue would be preferable to an S3 bucket.

INCORRECT: "Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic" is incorrect as notifications to topics are pushed to subscribers. In this case we want the second microservice to pickup the messages when ready (pull them).

INCORRECT: "Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose" is incorrect as this is not how Firehose works. Firehose sends data directly to destinations, it is not a message queue.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html>

QUESTION 34

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most.

The company wants to keep costs as low as possible by using the appropriate S3 storage class. Which S3 storage class should be implemented to meet these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. This is an ideal use case for intelligent-tiering as the access patterns for the log files are not known. CORRECT: "S3 Intelligent-Tiering" is the correct answer. INCORRECT: "S3 Standard-Infrequent Access (S3 Standard-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive. INCORRECT: "S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive. INCORRECT: "S3 Glacier" is incorrect as if the data is accessed often retrieval fees could become expensive. Glacier also requires more work in retrieving the data from the archive and quick access requirements can add further costs.

References: https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

QUESTION 35

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

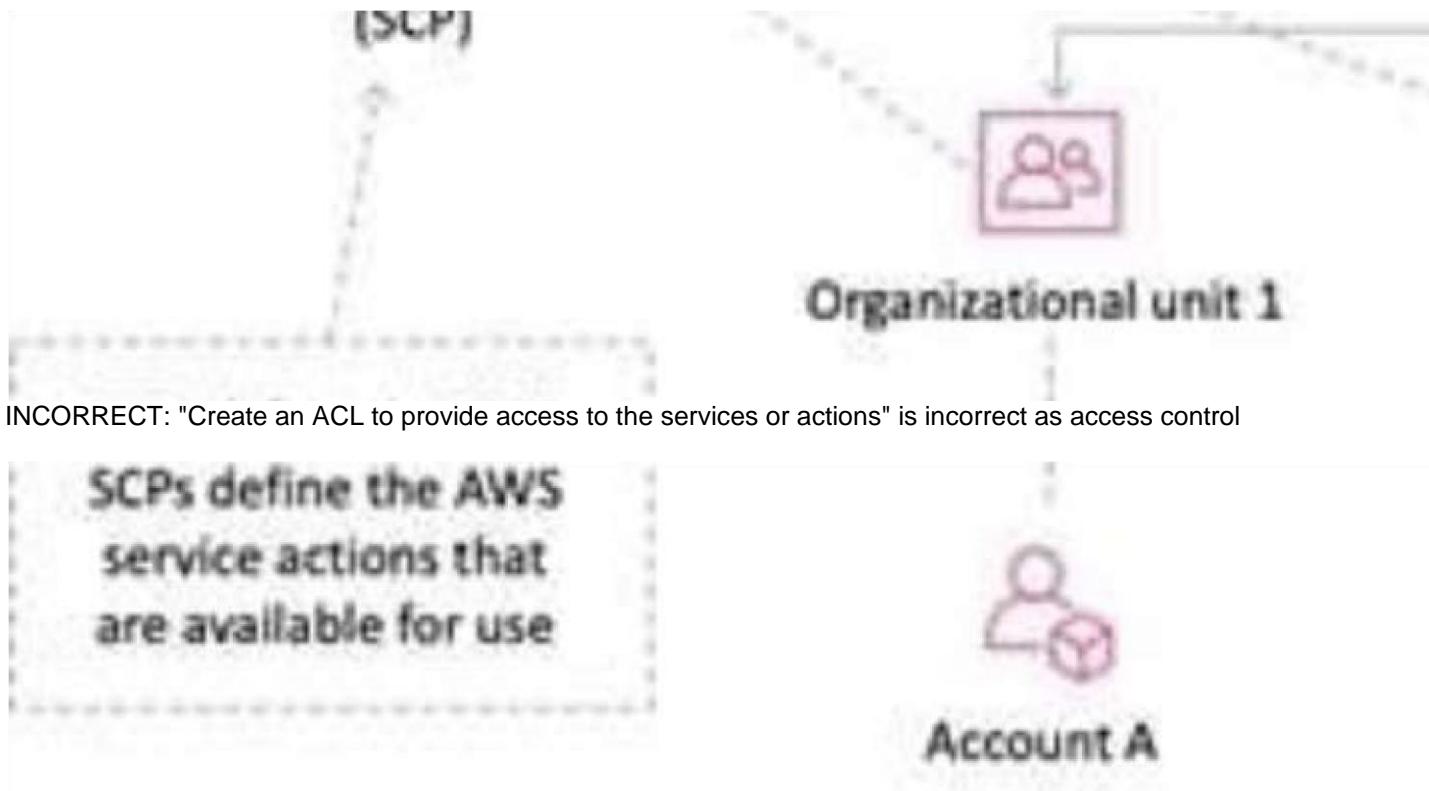
Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.

SCPs alone are not sufficient for allowing access in the accounts in your organization. Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a guardrail for what actions the principals can perform. You still need to attach identity-based or resource-based policies to principals or resources in your



organization's accounts to actually grant permissions to them.

CORRECT: "Create a service control policy in the root organizational unit to deny access to the services or actions" is the correct answer.



lists are not used for permissions associated with IAM. Permissions policies are used with IAM.
 INCORRECT: "Create a security group to allow accounts and attach it to user groups" is incorrect as security groups are instance level firewalls. They do not limit service actions. INCORRECT: "Create crossaccount roles in each account to deny access to the services or actions" is incorrect as this is a complex solution and does not provide centralized control References:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

QUESTION 36

You are trying to launch an EC2 instance, however the instance seems to go into a terminated status immediately. What would probably not be a reason that this is happening?

- A. The AMI is missing a required part.
- B. The snapshot is corrupt.
- C. You need to create storage in EBS first.
- D. You've reached your volume limit.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon EC2 provides a virtual computing environments, known as an instance. After you launch an instance, AWS recommends that you check its status to confirm that it goes from the pending status to the running status, the not terminated status. The following are a few reasons why an Amazon EBS-backed instance might immediately terminate:

You've reached your volume limit.

The AMI is missing a required part.

The snapshot is corrupt.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.html

QUESTION 37

You have set up an Auto Scaling group. The cool down period for the Auto Scaling group is 7 minutes. The first instance is launched after 3 minutes, while the second instance is launched after 4 minutes. How many minutes after the first instance is launched will Auto Scaling accept another scaling activity request?

- A. 11 minutes
- B. 7 minutes
- C. 10 minutes
- D. 14 minutes

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If an Auto Scaling group is launching more than one instance, the cool down period for each instance starts after that instance is launched. The group remains locked until the last instance that was launched has completed its cool down period. In this case the cool down period for the first instance starts after 3 minutes and finishes at the 10th minute (3+7 cool down), while for the second instance it starts at the 4th minute and finishes at the 11th minute (4+7 cool down). Thus, the Auto Scaling group will receive another request only after 11 minutes. Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

QUESTION 38

In Amazon EC2 Container Service components, what is the name of a logical grouping of container instances on which you can place tasks?

- A. A cluster
- B. A container instance
- C. A container
- D. A task definition

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon ECS contains the following components:

A Cluster is a logical grouping of container instances that you can place tasks on. A Container instance is an Amazon EC2 instance that is running the Amazon ECS agent and has been registered into a cluster. A Task definition is a description of an application that contains one or more container definitions. A Scheduler is the method used for placing tasks on container instances. A Service is an Amazon ECS service that allows you to run and maintain a specified number of instances of a task definition simultaneously.

A Task is an instantiation of a task definition that is running on a container instance. A Container is a Linux container that was created as part of a task. Reference: <http://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html>

QUESTION 39

In the context of AWS support, why must an EC2 instance be unreachable for 20 minutes rather than allowing customers to open tickets immediately?

- A. Because most reachability issues are resolved by automated processes in less than 20 minutes
- B. Because all EC2 instances are unreachable for 20 minutes every day when AWS does routine maintenance
- C. Because all EC2 instances are unreachable for 20 minutes when first launched

- D. Because of all the reasons listed here

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An EC2 instance must be unreachable for 20 minutes before opening a ticket, because most reachability issues are resolved by automated processes in less than 20 minutes and will not require any action on the part of the customer. If the instance is still unreachable after this time frame has passed, then you should open a case with support. Reference: <https://aws.amazon.com/premiumsupport/faqs/>

QUESTION 40 Can a user get a notification of each instance start / terminate configured with Auto Scaling?

- A. Yes, if configured with the Launch Config
- B. Yes, always
- C. Yes, if configured with the Auto Scaling group
- D. No

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The user can get notifications using SNS if he has configured the notifications while creating the Auto Scaling group.

Reference:

<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html>

QUESTION 41

Amazon EBS provides the ability to create backups of any Amazon EC2 volume into what is known as _____.

- A. snapshots
- B. images
- C. instance backups
- D. mirrors

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon allows you to make backups of the data stored in your EBS volumes through snapshots that can later be used to create a new EBS volume.

Reference: <http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html>

QUESTION 42

To specify a resource in a policy statement, in Amazon EC2, can you use its Amazon Resource Name (ARN)?

- A. Yes, you can.
- B. No, you can't because EC2 is not related to ARN.
- C. No, you can't because you can't specify a particular Amazon EC2 resource in an IAM policy.

D. Yes, you can but only for the resources that are not affected by the action.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Some Amazon EC2 API actions allow you to include specific resources in your policy that can be created or modified by the action. To specify a resource in the statement, you need to use its Amazon Resource Name (ARN).

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf>

QUESTION 43

After you recommend Amazon Redshift to a client as an alternative solution to paying data warehouses to analyze his data, your client asks you to explain why you are recommending Redshift. Which of the following would be a reasonable response to his request?

- A. It has high performance at scale as data and query complexity grows.
- B. It prevents reporting and analytic processing from interfering with the performance of OLTP workloads.
- C. You don't have the administrative burden of running your own data warehouse and dealing with setup, durability, monitoring, scaling, and patching.
- D. All answers listed are a reasonable response to his question

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon Redshift delivers fast query performance by using columnar storage technology to improve I/O efficiency and parallelizing queries across multiple nodes. Redshift uses standard PostgreSQL JDBC and ODBC drivers, allowing you to use a wide range of familiar SQL clients. Data load speed scales linearly with cluster size, with integrations to Amazon S3, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Kinesis or any SSH-enabled host. AWS recommends Amazon Redshift for customers who have a combination of needs, such as:

High performance at scale as data and query complexity grows
Desire to prevent reporting and analytic processing from interfering with the performance of OLTP workloads
Large volumes of structured data to persist and query using standard SQL and existing BI tools
Desire to the administrative burden of running one's own data warehouse and dealing with setup, durability, monitoring, scaling and patching

Reference: https://aws.amazon.com/running_databases/#redshift_anchor

QUESTION 44

One of the criteria for a new deployment is that the customer wants to use AWS Storage Gateway.

However you are not sure whether you should use gateway-cached volumes or gateway-stored volumes or even what the differences are. Which statement below best describes those differences?

- A. Gateway-cached lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.
Gateway-stored enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.
- B. Gateway-cached is free whilst gateway-stored is not.
- C. Gateway-cached is up to 10 times faster than gateway-stored.
- D. Gateway-stored lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.

Gateway-cached enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.

Correct Answer: A

Section: (none)**Explanation****Explanation/Reference:**

Explanation:

Volume gateways provide cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers. The gateway supports the following volume configurations:

Gateway-cached volumes ?You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Gateway-cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on- premises. You also retain lowlatency access to your frequently accessed data. Gateway-stored volumes ?If you need low-latency access to your entire data set, you can configure your on- premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive off-site backups that you can recover to your local data center or Amazon EC2.

For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2. Reference:

<http://docs.aws.amazon.com/storagegateway/latest/userguide/volumegateway.html>

QUESTION 45

A user is launching an EC2 instance in the US East region. Which of the below mentioned options is recommended by AWS with respect to the selection of the availability zone?

- A. Always select the AZ while launching an instance
- B. Always select the US-East-1-a zone for HA
- C. Do not select the AZ; instead let AWS select the AZ
- D. The user can never select the availability zone while launching an instance

Correct Answer: C**Section: (none)****Explanation****Explanation/Reference:**

Explanation:

When launching an instance with EC2, AWS recommends not to select the availability zone (AZ). AWS specifies that the default Availability Zone should be accepted. This is because it enables AWS to select the best Availability Zone based on the system health and available capacity. If the user launches additional instances, only then an Availability Zone should be specified. This is to specify the same or different AZ from the running instances. Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usingregions-availability-zones.html>

QUESTION 46

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content Users around the globe are reporting that the website is slow.

Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin.
Then update the Amazon Route 53 record to point to the CloudFront distribution.
- B. Create a latency-based Amazon Route 53 record for the ALB.
Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users.Then register the instances with the same ALB using cross-Region VPC peering.
- D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB andEC2 instances.
Then update an Amazon Route 53 record to point to the S3 buckets.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon CloudFront is a content delivery network (CDN) that improves website performance by caching content at edge locations around the world. It can serve both dynamic and static content.

This is the best solution for improving the performance of the website. CORRECT: "Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution" is the correct answer. INCORRECT: "Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB" is incorrect. Latency routing routes based on the latency between the client and AWS. There is no mention in the answer about creating the new instances in another region therefore the only advantage is in using larger instance sizes. For a dynamic site this adds complexity in keeping the instances in sync.

INCORRECT: "Launch new EC2 instances hosting the same web application in different Regions closer to the users. Use an AWS Transit Gateway to connect customers to the closest region" is incorrect as Transit Gateway is a service for connecting on-premises networks and VPCs to a single gateway.

INCORRECT: "Migrate the website to an Amazon S3 bucket in the Regions closest to the users. Then create an Amazon Route 53 geolocation record to point to the S3 buckets" is incorrect as with S3 you can only host static websites, not dynamic websites.

References: <https://aws.amazon.com/cloudfront/dynamic-content/>

QUESTION 47

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud.

The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application and more economical cold storage to hold the data when the application is not actively running. Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage

- E. Amazon FSx for Windows for high-performance parallel storage

Correct Answer: AD

Section: (none)

Explanation

Availability Zone

Explanation/Reference:

Public subnet

Explanation:

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads

such as machine learning, high-performance computing (HPC), video processing, financial modeling, and

electronic design automation (EDA). These workloads commonly require data to be presented via a fast

EC2 Instance

Amazon FSx

and scalable file system interface, and typically have data sets stored on long-term data stores like

Amazon S3.

Availability Zone

Public subnet



Amazon FSx works natively with Amazon S3, making it easy to access your S3 data to run data processing



workloads. Your S3 objects are presented as files in your file system, and you can write your results back

EC2 Instance

to S3. This lets you run data processing workloads on FSx for Lustre and store your long-term data on S3



or on-premises data stores. Therefore, the best combination for this scenario is to use S3 for cold data and



FSx for Lustre for the parallel HPC job.

CORRECT: "Amazon S3 for cold data storage" is the correct answer. CORRECT: "Amazon FSx for Lustre for high-performance parallel storage" is the correct answer. INCORRECT: "Amazon EFS for cold data storage" is incorrect as FSx works natively with S3 which is also more economical.

INCORRECT: "Amazon S3 for high-performance parallel storage" is incorrect as S3 is not suitable for running high-performance computing jobs. INCORRECT: "Amazon FSx for Windows for high-performance parallel storage" is incorrect as FSx for Lustre should be used for HPC use cases and use cases that require storing data on S3.

References:

<https://aws.amazon.com/fsx/lustre/>

QUESTION 48

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: <https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/> **QUESTION 49**

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that

performs faster and provides high availability using data replication. Which database should a solutions architect recommend?

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

Correct Answer: C

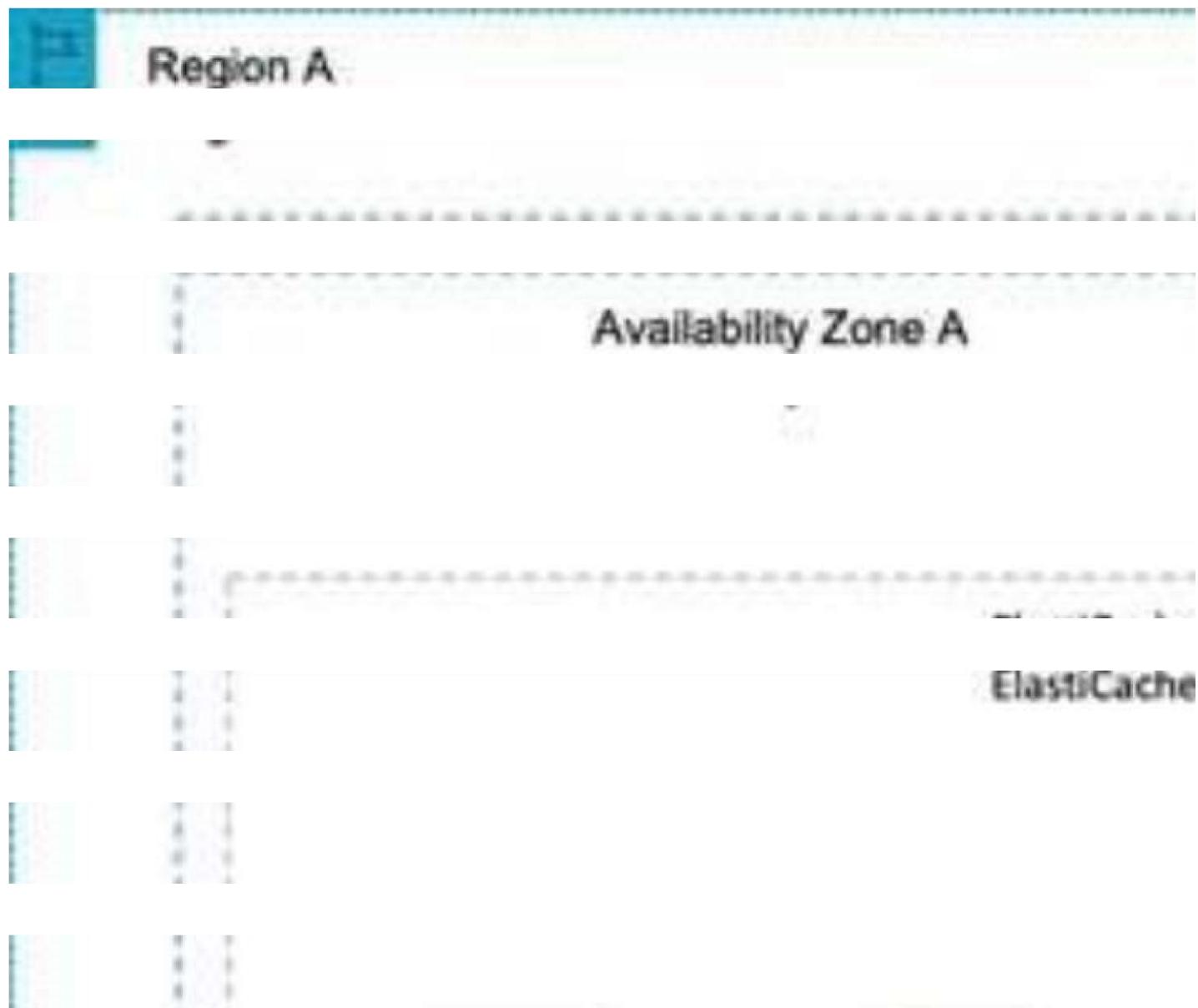
Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon ElastiCache is an in-memory database. With ElastiCache Memcached there is no data replication or high availability. As you can see in the diagram, each node is a separate partition of data:



Region A

Availability Zone A

Shard

Primary



Replica 1 Replica 2

Shard

Primary



Replica 1 Replica 2

following diagram shows a Redis architecture with cluster mode enabled:



CORRECT: "Amazon ElastiCache for Redis" is the correct answer. INCORRECT: "Amazon ElastiCache for Memcached" is incorrect as Memcached does not support data replication or high availability.

INCORRECT: "Amazon RDS for MySQL" is incorrect as this is not an in-memory database. INCORRECT: "Amazon RDS for PostgreSQL" is incorrect as this is not an in-memory database.

References:

<https://aws.amazon.com/elasticsearch/redis/>

QUESTION 50

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer.

Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users. Which solution will meet these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. AWS Auto Scaling refers to a collection of Auto Scaling capabilities across several AWS services.

The services within the AWS Auto Scaling family include:

Amazon EC2 (known as Amazon EC2 Auto Scaling).

■

Amazon ECS.

■

Amazon DynamoDB.

■

Amazon Aurora.

■

The scaling options define the triggers and when instances should be provisioned/de-provisioned.

There are four scaling options:

Maintain keep a specific or minimum number of instances running.

■

Manual use maximum, minimum, or a specific number of instances.

■

Scheduled increase or decrease the number of instances based on a schedule.

■

Dynamic scale based on real-time system metrics (e.g. CloudWatch metrics).

■

The following table describes the scaling options available and when to use them:

Scaling	
Maintain	Ensures the instances
Manual	Manually

via the co

Scheduled

The scaling options are configured through Scaling Policies which determine when, if, and how the ASG

scales and shrinks.

Adjust min

specific da

time perio

The following table describes the scaling policy types available for dynamic scaling policies and when to

Dynamic

use them (more detail further down the page):

Scale in re

other trig

Scaling Policy

Wha

Target Tracking	The scaling policy monitors the target metric and scales the capacity as required to meet the target.
Target Tracking	The scaling policy monitors the target metric and scales the capacity as required to meet the target.
Policy	capacity as required
	at, or close to, the target value
Simple Scaling	Wait until health metric reaches threshold
Simple Scaling	Wait until health metric reaches threshold
Policy	down period expires
	or application goes down

The diagram below depicts an Auto Scaling group with a Scaling policy set to a minimum size of 1

evaluating

instance, a desired capacity of 2 instances, and a maximum size of 4 instances:

Amazon EC2 Auto Scaling supports sending Amazon SNS notifications when the following events occur.

QUESTION 51

Step Scaling Policy

A company has a two-tier application architecture that runs in public and private subnets Amazon EC2

instances running the web application are in the public subnet and a database runs on the private subnet.

capacity of your Au

The web application instances and the database are running in a single Availability Zone (AZ). Which

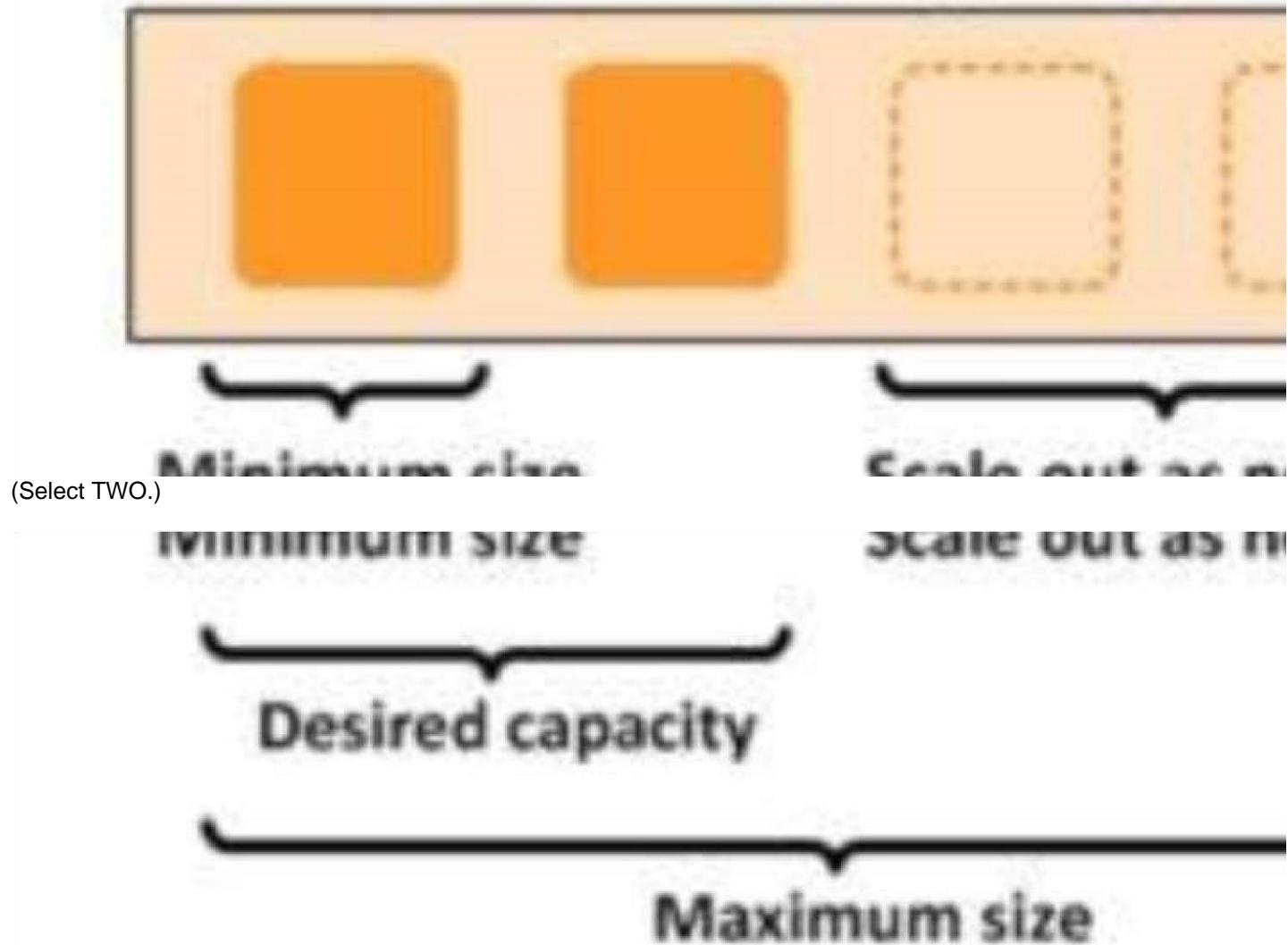
combination of steps should a solutions architect take to provide high availability for this architecture?

based on a set of s

known as step adj

known as step adj

Auto Scaling group



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

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You would like the EC2 instances to have high availability by placing them in multiple AZs.

QUESTION 52

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

Which changes should be made to the database tier to improve performance?

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

Correct Answer: D

Section: (none)

Explanation

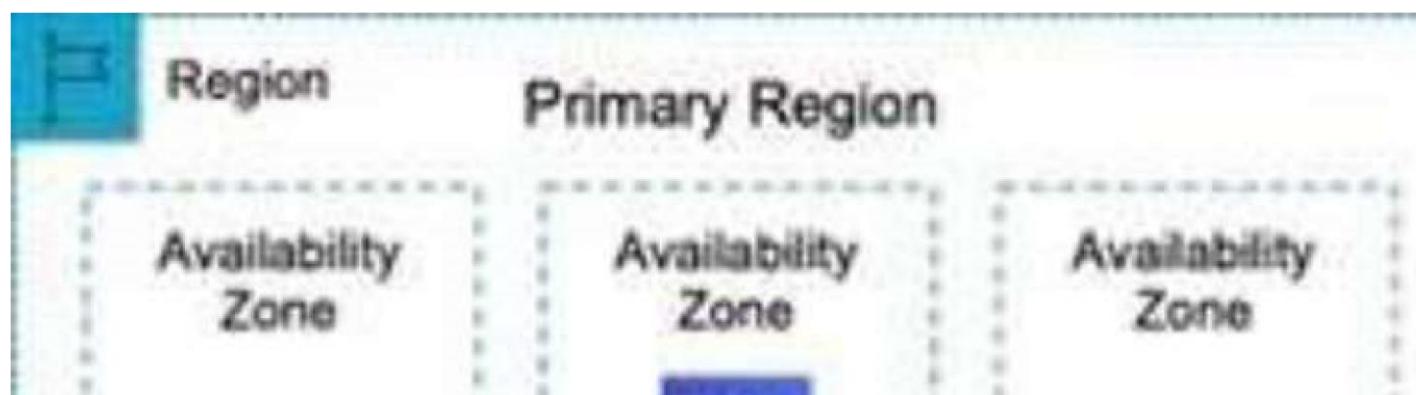
Explanation/Reference:

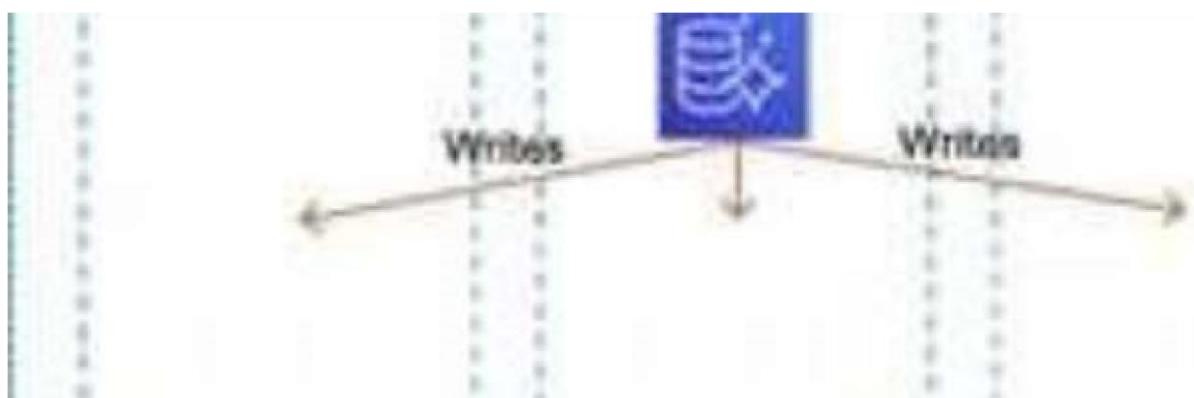
Explanation:

The issue here is latency with read queries being directed from Australia to UK which is great physical distance. A solution is required for improving read performance in Australia. An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only, secondary AWS Regions.

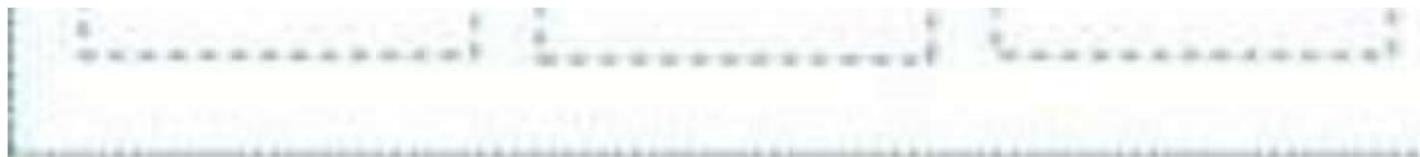
Aurora replicates data to the secondary AWS Regions with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS Region.

This solution will provide better performance for users in the Australia Region for queries. Writes must still take place in the UK Region but read performance will be greatly improved. CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2" is the correct answer. INCORRECT: "Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region" is incorrect. The database is located in UK. If the database is migrated to Australia then the reverse problem will occur. Multi-AZ does not assist with improving query performance across Regions.





INCORRECT: "Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable



replication to additional Regions" is incorrect as a relational database running on MySQL is unlikely to be

compatible with DynamoDB.

INCORRECT: "Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance" is incorrect as you can only put ALBs in front of the web tier, not the DB tier.

References: <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

QUESTION 53

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier. The solution must avoid saturating the branch office's lowbandwidth internet connection.

What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Create a bucket policy to enforce a VPC endpoint.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint.

- C. Mount the network-attached file system to Amazon S3 and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- D. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

As the company's internet link is low-bandwidth uploading directly to Amazon S3 (ready for transition to Glacier) would saturate the link. The best alternative is to use AWS Snowball appliances. The Snowball edge appliance can hold up to 75 TB of data so 10 devices would be required to migrate 750 TB of data. Snowball moves data into AWS using a hardware device and the data is then copied into an Amazon S3 bucket of your choice. From there, lifecycle policies can transition the S3 objects to Amazon S3 Glacier.

CORRECT: "Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination.

Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier" is the correct answer.

INCORRECT: "Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination.

Create a bucket policy to enforce a VPC endpoint" is incorrect as you cannot set a Glacier vault as the destination, it must be an S3 bucket. You also can't enforce a VPC endpoint using a bucket policy.

INCORRECT: "Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier" is incorrect as this is not the most cost- effective option and takes time to setup.

INCORRECT: "Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth" is incorrect as this service is not used for accelerating or optimizing the upload of data from on-premises networks. References: <https://docs.aws.amazon.com/snowball/latest/developer-guide/specifications.html>

QUESTION 54

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance.

The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application. How can this be achieved?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

CORRECT: "Create a Multi-AZ RDS Read Replica of the production RDS DB instance" is the correct answer.

INCORRECT: "Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica" is incorrect. Read replicas are primarily used for horizontal scaling. The best solution for high availability is to use a Multi-AZ read replica.

INCORRECT: "Create a cross-region Multi-AZ deployment and create a read replica in the second region" is incorrect as you cannot create a cross- region Multi-AZ deployment with RDS. INCORRECT: "Use Amazon Data Lifecycle Manager to automatically create and manage snapshots" is incorrect as using snapshots is not the best solution for high availability.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_SQLReplication.html#USER_SQLReplication.ReadReplicas.MultiAZ

QUESTION 55

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility.

However the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies. How should a solutions architect address this issue?

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

Correct Answer: D

Section: (none)

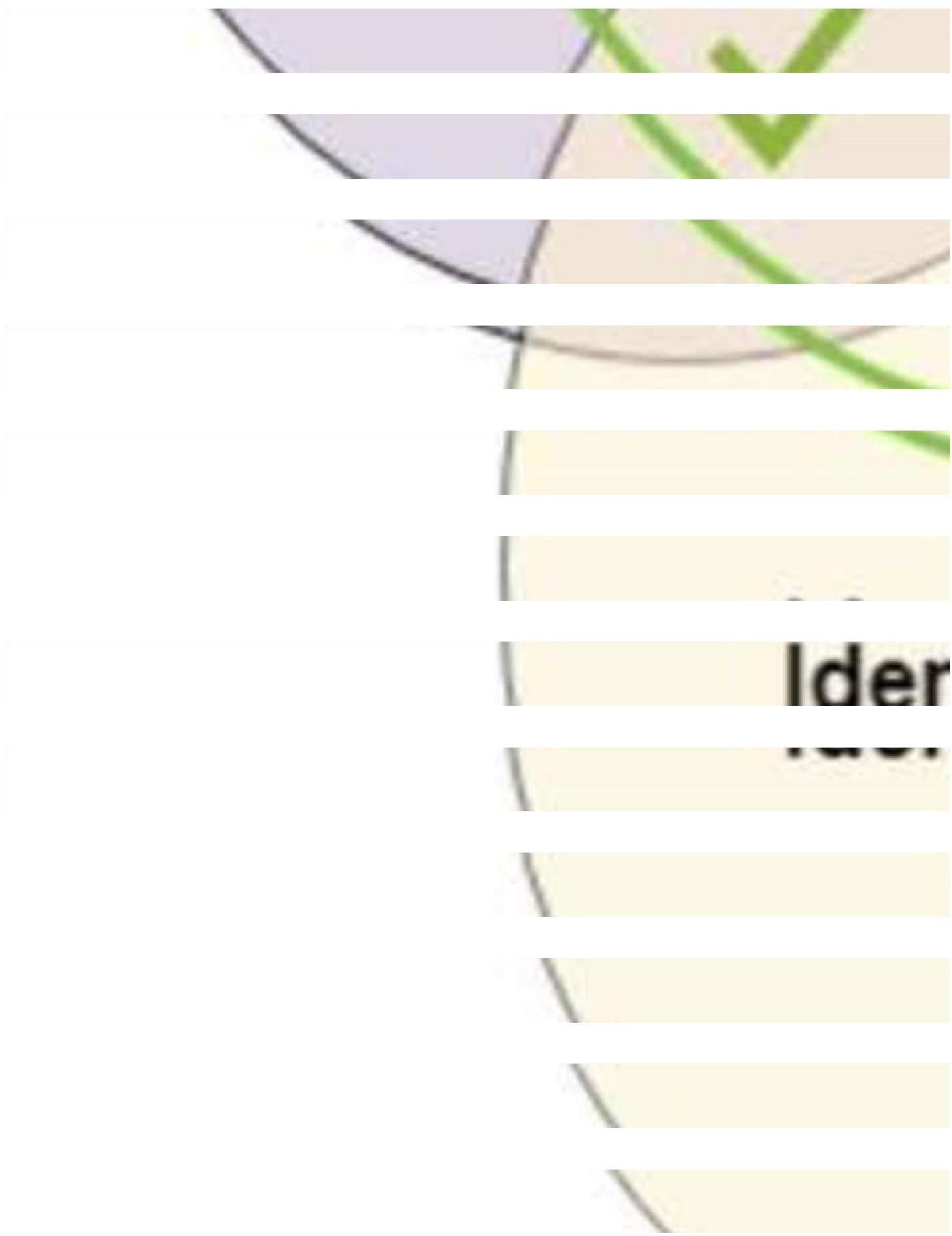
Explanation

Explanation/Reference:

Explanation:

The permissions boundary for an IAM entity (user or role) sets the maximum permissions that the entity can have. This can change the effective permissions for that user or role. The effective permissions for an entity are the permissions that are granted by all the policies that affect the user or role. Within an account, the permissions for an entity can be affected by identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, or session policies.

Resource-based policy



Therefore, the solutions architect can set an IAM permissions boundary on the developer IAM role that

explicitly denies attaching the administrator policy. CORRECT: "Set an IAM permissions boundary on the

developer IAM role that explicitly denies attaching the administrator policy" is the correct answer.

INCORRECT: "Create an Amazon SNS topic to send an alert every time a developer creates a new policy"

is incorrect as this would mean investigating every incident which is not an efficient solution.

INCORRECT: "Use service control policies to disable IAM activity across all accounts in the organizational unit" is incorrect as this would prevent the developers from being able to work with IAM completely.

INCORRECT: "Prevent the developers from attaching any policies and assign all IAM duties to the security operations team" is incorrect as this is not necessary. The requirement is to allow developers to work with policies, the solution needs to find a secure way of achieving this.

References:

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

QUESTION 56

A user is storing a large number of objects on AWS S3. The user wants to implement the search functionality among the objects. How can the user achieve this?

- A. Use the indexing feature of S3.
- B. Tag the objects with the metadata to search on that.
- C. Use the query functionality of S3.
- D. Make your own DB system which stores the S3 metadata for the search functionality.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In Amazon Web Services, AWS S3 does not provide any query facility. To retrieve a specific object the user needs to know the exact bucket / object key. In this case it is recommended to have an own DB system which manages the S3 metadata and key mapping. Reference:

http://media.amazonwebservices.com/AWS_Storage_Options.pdf

QUESTION 57

After setting up a Virtual Private Cloud (VPC) network, a more experienced cloud engineer suggests that to achieve low network latency and high network throughput you should look into setting up a placement group. You know nothing about this, but begin to do some research about it and are especially curious about its limitations. Which of the below statements is wrong in describing the limitations of a placement group?

- A. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed.
- B. A placement group can span multiple Availability Zones.
- C. You can't move an existing instance into a placement group.
- D. A placement group can span peered VPCs

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gbps network. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.

Placement groups have the following limitations:

The name you specify for a placement group a name must be unique within your AWS account. A placement group can't span multiple Availability Zones. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed. We recommend using the same instance type for all instances in a placement group. You can't merge placement groups. Instead, you must terminate the instances in one placement group, and then relaunch those instances into the other placement group. A placement group can span peered VPCs; however, you will not get full- bisection bandwidth between instances in peered VPCs. For more information about VPC peering connections, see VPC Peering in the Amazon VPC User Guide. You can't move an existing instance into a placement group. You can create an AMI from your existing instance, and then launch a new instance from the AMI into a placement group. Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Exam B

QUESTION 1

What is a placement group in Amazon EC2?

- A. It is a group of EC2 instances within a single Availability Zone.
- B. It is the edge location of your web content.
- C. It is the AWS region where you run the EC2 instance of your web content.
- D. It is a group used to span multiple Availability Zones.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A placement group is a logical grouping of instances within a single Availability Zone. Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

QUESTION 2

You are migrating an internal server on your DC to an EC2 instance with EBS volume. Your server disk usage is around 500GB so you just copied all your data to a 2TB disk to be used with AWS Import/Export. Where will the data be imported once it arrives at Amazon?

- A. to a 2TB EBS volume
- B. to an S3 bucket with 2 objects of 1TB
- C. to an 500GB EBS volume
- D. to an S3 bucket as a 2TB snapshot

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An import to Amazon EBS will have different results depending on whether the capacity of your storage device is less than or equal to 1 TB or greater than 1 TB. The maximum size of an Amazon EBS snapshot is 1 TB, so if the device image is larger than 1 TB, the image is chunked and stored on Amazon S3. The target location is determined based on the total capacity of the device, not the amount of data on the device.

Reference: <http://docs.aws.amazon.com/AWSImportExport/latest/DG/Concepts.html>

QUESTION 3

A client needs you to import some existing infrastructure from a dedicated hosting provider to AWS to try and save on the cost of running his current website. He also needs an automated process that manages backups, software patching, automatic failure detection, and recovery. You are aware that his existing set up currently uses an Oracle database. Which of the following AWS databases would be best for accomplishing this task?

- A. Amazon RDS
- B. Amazon Redshift
- C. Amazon SimpleDB
- D. Amazon ElastiCache

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon RDS gives you access to the capabilities of a familiar MySQL, Oracle, SQL Server, or PostgreSQL database engine. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS. Amazon RDS automatically patches the database software and backs up your database, storing the backups for a user-defined retention period and enabling point-in-time recovery. Reference: <http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide>Welcome.html>

QUESTION 4 True or false: A VPC contains multiple subnets, where each subnet can span multiple Availability Zones.

- A. This is true only if requested during the set-up of VPC.
- B. This is true.
- C. This is false.
- D. This is true only for US regions.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A VPC can span several Availability Zones. In contrast, a subnet must reside within a single Availability Zone.

Reference: <https://aws.amazon.com/vpc/faqs/>

QUESTION 5 An edge location refers to which Amazon Web Service?

- A. An edge location is referred to the network configured within a Zone or Region
- B. An edge location is an AWS Region
- C. An edge location is the location of the data center used for Amazon CloudFront.
- D. An edge location is a Zone within an AWS Region

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon CloudFront is a content distribution network. A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers across the world. The location of the data center used for CDN is called edge location. Amazon CloudFront can cache static content at each edge location. This means that your popular static content (e.g., your site's logo, navigational images, cascading style sheets, JavaScript code, etc.) will be available at a nearby edge location for the browsers to download with low latency and improved performance for viewers. Caching popular static content with Amazon CloudFront also helps you offload requests for such files from your origin sever - CloudFront serves the cached copy when available and only makes a request to your origin server if the edge location receiving the browser's request does not have a copy of the file.

Reference: <http://aws.amazon.com/cloudfront/>

QUESTION 6

You are looking at ways to improve some existing infrastructure as it seems a lot of engineering resources are being taken up with basic management and monitoring tasks and the costs seem to be excessive. You are thinking of deploying Amazon ElasticCache to help. Which of the following statements is true in regards to ElasticCache?

- A. You can improve load and response times to user actions and queries however the cost associated with scaling web applications will be more.
- B. You can't improve load and response times to user actions and queries but you can reduce the cost associated with scaling web applications.
- C. You can improve load and response times to user actions and queries however the cost associated with scaling web applications will remain the same.
- D. You can improve load and response times to user actions and queries and also reduce the cost associated with scaling web applications.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory caching system, instead of relying entirely on slower disk-based databases. The service simplifies and offloads the management, monitoring and operation of in-memory cache environments, enabling your engineering resources to focus on developing applications. Using Amazon ElastiCache, you can not only improve load and response times to user actions and queries, but also reduce the cost associated with scaling web applications. Reference: <https://aws.amazon.com/elasticsearch/faqs/>

QUESTION 7 Do Amazon EBS volumes persist independently from the running life of an Amazon EC2 instance?

- A. Yes, they do but only if they are detached from the instance.
- B. No, you cannot attach EBS volumes to an instance.
- C. No, they are dependent.
- D. Yes, they do.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An Amazon EBS volume behaves like a raw, unformatted, external block device that you can attach to a single instance. The volume persists independently from the running life of an Amazon EC2 instance.

Reference: <http://docs.amazonaws.com/AWSEC2/latest/UserGuide/Storage.html>

QUESTION 8

Your supervisor has asked you to build a simple file synchronization service for your department. He doesn't want to spend too much money and he wants to be notified of any changes to files by email. What do you think would be the best Amazon service to use for the email solution?

- A. Amazon SES
- B. Amazon CloudSearch
- C. Amazon SWF
- D. Amazon AppStream

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

File change notifications can be sent via email to users following the resource with Amazon Simple Email Service (Amazon SES), an easy-to-use, cost-effective email solution.

Reference:

http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_filesync_08.pdf

QUESTION 9

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months.

Which set of actions should a solutions architect take to support these needs'?

- A. Store the data in an Amazon EBS volume.
Mount the EBS volume on the application instances
- B. Store the data in an Amazon EFS file system.
Mount the file system on the application instances.
- C. Store the data in Amazon S3 Glacier.
Update the vault policy to allow access to the application instances.
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Update the bucket policy to allow access to the application instances.

Correct Answer: B**Section: (none)****Explanation****Explanation/Reference:****Explanation:**

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. "It is built to scale on demand to petabytes without disrupting applications", "growing and shrinking automatically as you add and remove files", eliminating the need to provision and manage capacity to accommodate growth. "The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances."

QUESTION 10

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.

What should a solutions architect do to meet these requirements? (Select TWO.)

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

Correct Answer: CE**Section: (none)****Explanation****Explanation/Reference:****Explanation:**

The solutions architect must enable high availability for the architecture and ensure it is cost-effective. To enable high availability an Amazon EC2 Auto Scaling group should be created to add and remove instances across multiple availability zones. In order to distribute the traffic to the instances the architecture should use a Network Load Balancer which operates at Layer 4. This architecture will also be cost-effective as the Auto Scaling group will ensure the right number of instances are running based on demand.

CORRECT:

"Configure a Network Load Balancer in front of the EC2 instances" is a correct answer.

CORRECT: "Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically" is also a correct answer.

INCORRECT: "Increase the number of instances and use smaller EC2 instance types" is incorrect as this is not the most cost-effective option. Auto Scaling should be used to maintain the right number of active instances.

INCORRECT: "Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically" is incorrect as this is not highly available as it's a single AZ. INCORRECT: "Configure an Application Load Balancer in front of the EC2 instances" is incorrect as an ALB operates at Layer 7 rather than Layer 4.

References: <https://docsaws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>

QUESTION 11

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue. Occasional duplicate records are found in the RDS table.

The SQS queue does not contain any duplicate messages. What should a solutions architect do to ensure messages are being processed once only?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Keyword: SQS queue writes to an Amazon RDS

From this, Option D best suits & other Options ruled out [Option A - You can't introduce one more Queue in the existing one; Option B - only Permission & Option C - Only Retrieves Messages]

FIFO queues are designed to never introduce duplicate messages. However, your message producer

At-Least-Once Delivery: A message is delivered at least once, but it may be delivered more than once. This means that occasionally more than one copy of a message is delivered to a consumer.

Best-Effort Ordering: Occasionally, messages might be delivered out of order or not at all.

might introduce duplicates in certain scenarios: for example, if the producer sends a message, does not receive a response, and then resends the same message. Amazon SQS APIs provide deduplication functionality that prevents your message producer from sending duplicates. Any duplicates introduced by the message producer are removed within a 5-minute deduplication interval.

For standard queues, you might occasionally receive a duplicate copy of a message (at-least- once delivery). If you use a standard queue, you must design your applications to be idempotent (that is, they must not be affected adversely when processing the same message more than once).

CreateQueue - You can't change the queue type after you create it and you can't convert an existing standard queue into a FIFO queue. You must either create a new FIFO queue for your application or delete your existing standard queue and recreate it as a FIFO queue.

AddPermission - You create a queue, you have full control access rights for the queue. Only you, the owner of the queue, can grant or deny permissions to the queue.

ReceiveMessage - Retrieves one or more messages (up to 10), from the specified queue.

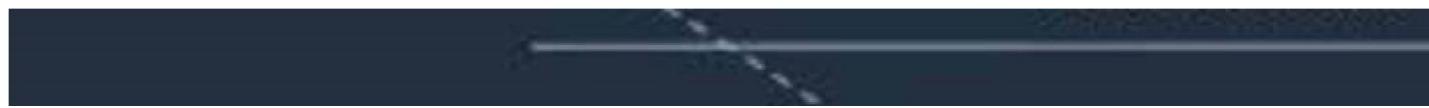
FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it.

in an order different from which they were sent.

Amazon SQS Visibility Timeout



SQS Queue



Producer

Delay Seconds

Delay Seconds

Timeline



References:

https://aws.amazon.com/sqs/?nc2=h_ql_prod_ap_sqs

<https://aws.amazon.com/sqs/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html#FIFO-queues-exactly-once-processing> <https://youtu.be/XrX7rb6M3jw>

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_ChangeMessageVisibility.html

geVisibility.html

QUESTION 12 A solutions architect is designing an application for a two-step order process.

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html> "Standard queues provide at-least-once delivery, which means that each message is delivered at least once.

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. Duplicates are not introduced into the queue."

QUESTION 13

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

Which EC2 configuration meets these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload.

Depending on the type of workload, you can create a placement group using one of the following placement strategies:

Cluster - packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications. Partition - spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.

Spread - strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

For this scenario, a cluster placement group should be used as this is the best option for providing low-latency network performance for a HPC application. CORRECT: "Launch the EC2 instances in a cluster placement group in one Availability Zone" is the correct answer.

INCORRECT: "Launch the EC2 instances in a spread placement group in one Availability Zone" is incorrect as the spread placement group is used to spread instances across distinct underlying hardware.

INCORRECT: "Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances" is incorrect as this does not achieve the stated requirement to provide low-latency, high throughput network performance between instances.

Also, you cannot use an ELB across Regions.

INCORRECT: "Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones" is incorrect as this does not reduce network latency or improve performance.

References: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

QUESTION 14

A company is planning to use Amazon S3 to store images uploaded by its users.

The images must be encrypted at rest in Amazon S3.

The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS. You can choose a customer managed CMK or the AWS managed CMK for Amazon S3 in your account.

Customer managed CMKs are CMKs in your AWS account that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the CMK, and scheduling the CMKs for deletion. For this scenario, the solutions architect should use SSE-KMS with a customer managed CMK. That way KMS will manage the data key but the company can configure key policies defining who can access the keys.

CORRECT: "Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)" is the correct answer.

INCORRECT: "Server-Side Encryption with keys stored in an S3 bucket" is incorrect as you cannot store your keys in a bucket with server-side encryption

INCORRECT: "Server-Side Encryption with CustomerProvided Keys (SSE-C)" is incorrect as the company does not want to manage the keys.

INCORRECT: "Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)" is incorrect as the company needs to manage access control for the keys which is not possible when they're managed by Amazon.

References: <https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse>

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

QUESTION 15

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

{
several users.

"Version": "2012-1

"Statement": [

 "Effect": "L

{

"Effect"

"Action"

"Resource"

"Condition"

"Communication"

"Work"

"Input"

}

}

1

2
3

{

"Effect"

"Action"

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.1001 in the us-east-1 Region.C.

Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is

10.100.100.254.

- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is

10.100.100.254.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

What the policy means:

1. Allow termination of any instance if user's source ip address is 10.100.100.254.
2. Deny termination of instances that are not in the us-east-1 region.

Combining this two, you get:

"Allow instance termination in the us-east-1 region if the user's source ip address is 10.100.100.254. Deny termination operation on other regions."

QUESTION 16

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Does DynamoDB support in-place atomic updates?

- A. Yes
- B. No
- C. It does support in-place non-atomic updates
- D. It is not defined

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

DynamoDB supports in-place atomic updates.

Reference:

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithItems.html#WorkingWithItems.AtomicCounters>

QUESTION 18

Your manager has just given you access to multiple VPN connections that someone else has recently set up between all your company's offices. She needs you to make sure that the communication between the VPNs is secure. Which of the following services would be best for providing a low-cost hub-and-spoke model for primary or backup connectivity between these remote offices?

- A. Amazon CloudFront
- B. AWS Direct Connect
- C. AWS CloudHSM
- D. AWS VPN CloudHub

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who would like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices. Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

QUESTION 19 Amazon EC2 provides a _____. It is an HTTP or HTTPS request that uses the HTTP verbs GET or POST.

- A. web database
- B. .net framework
- C. Query API
- D. C library

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon EC2 provides a Query API. These requests are HTTP or HTTPS requests that use the HTTP verbs GET or POST and a Query parameter named Action. Reference: <http://docs.aws.amazon.com/AWSEC2/latest/APIReference/making-api-requests.html>

QUESTION 20 In Amazon AWS, which of the following statements is true of key pairs?

- A. Key pairs are used only for Amazon SDKs.
- B. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
- C. Key pairs are used only for Elastic Load Balancing and AWS IAM.
- D. Key pairs are used for all Amazon services.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Key pairs consist of a public and private key, where you use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.

Reference: <http://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

QUESTION 21

Does Amazon DynamoDB support both increment and decrement atomic operations?

- A. Only increment, since decrement are inherently impossible with DynamoDB's data model.
- B. No, neither increment nor decrement operations.
- C. Yes, both increment and decrement operations.
- D. Only decrement, since increment are inherently impossible with DynamoDB's data model.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon DynamoDB supports increment and decrement atomic operations.

Reference:

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/APISummary.html>

QUESTION 22

An organization has three separate AWS accounts, one each for development, testing, and production.

The organization wants the testing team to have access to certain AWS resources in the production account. How can the organization achieve this?

- A. It is not possible to access resources of one account with another account.
- B. Create the IAM roles with cross account access.
- C. Create the IAM user in a test account, and allow it access to the production environment with the IAMpolicy.
- D. Create the IAM users with cross account access.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An organization has multiple AWS accounts to isolate a development environment from a testing or production environment. At times the users from one account need to access resources in the other account, such as promoting an update from the development environment to the production environment. In this case the IAM role with cross account access will provide a solution. Cross account access lets one account share access to their resources with users in the other AWS accounts.

Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 23

You need to import several hundred megabytes of data from a local Oracle database to an Amazon RDS DB instance. What does AWS recommend you use to accomplish this?

- A. Oracle export/import utilities
- B. Oracle SQL Developer
- C. Oracle Data Pump
- D. DBMS_FILE_TRANSFER

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

How you import data into an Amazon RDS DB instance depends on the amount of data you have and the number and variety of database objects in your database. For example, you can use Oracle SQL Developer to import a simple, 20 MB database; you want to use Oracle Data Pump to import complex databases or databases that are several hundred megabytes or several terabytes in size.

Reference:

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Oracle.Procedural.Importing.html>

QUESTION 24

A user has created an EBS volume with 1000 IOPS. What is the average IOPS that the user will get for most of the year as per EC2 SLA if the instance is attached to the EBS optimized instance?

- A. 950
- B. 990
- C. 1000

D. 900

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

As per AWS SLA if the instance is attached to an EBS-Optimized instance, then the Provisioned IOPS volumes are designed to deliver within 10% of the provisioned IOPS performance 99.9% of the time in a given year. Thus, if the user has created a volume of 1000 IOPS, the user will get a minimum 900 IOPS 99.9% time of the year.

Reference: <http://aws.amazon.com/ec2/faqs/>

QUESTION 25

You need to migrate a large amount of data into the cloud that you have stored on a hard disk and you decide that the best way to accomplish this is with AWS Import/Export and you mail the hard disk to AWS. Which of the following statements is incorrect in regards to AWS Import/Export?

- A. It can export from Amazon S3
- B. It can Import to Amazon GlacierC. It can export from Amazon Glacier.
- D. It can Import to Amazon EBS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AWS Import/Export supports:

Import to Amazon S3

Export from Amazon S3

Import to Amazon EBS

Import to Amazon Glacier

AWS Import/Export does not currently support export from Amazon EBS or Amazon Glacier. Reference: <https://docs.aws.amazon.com/AWSImportExport/latest/DG/whatisdisk.html>

QUESTION 26

You are in the process of creating a Route 53 DNS failover to direct traffic to two EC2 zones. Obviously, if one fails, you would like Route 53 to direct traffic to the other region. Each region has an ELB with some instances being distributed. What is the best way for you to configure the Route 53 health check?

- A. Route 53 doesn't support ELB with an internal health check. You need to create your own Route 53 health check of the ELB
- B. Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" off and "Associate with Health Check" on and R53 will use the ELB's internal health check.
- C. Route 53 doesn't support ELB with an internal health check. You need to associate your resourcerecord set for the ELB with your own health check
- D. Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" on and "Associate with Health Check" off and R53 will use the ELB's internal health check.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

With DNS Failover, Amazon Route 53 can help detect an outage of your website and redirect your end users to alternate locations where your application is operating properly. When you enable this feature, Route 53 uses health checks--regularly making Internet requests to your application's endpoints from multiple locations around the world--to determine whether each endpoint of your application is up or down. To enable DNS Failover for an ELB endpoint, create an Alias record pointing to the ELB and set the "Evaluate Target Health" parameter to true. Route 53 creates and manages the health checks for your ELB automatically. You do not need to create your own Route 53 health check of the ELB. You also do not need to associate your resource record set for the ELB with your own health check, because Route 53 automatically associates it with the health checks that Route 53 manages on your behalf. The ELB health check will also inherit the health of your backend instances behind that ELB. Reference: <http://aws.amazon.com/about-aws/whats-new/2013/05/30/amazon-route-53-adds-elb-integration-for-dnsfailover/>

QUESTION 27

A user wants to use an EBS-backed Amazon EC2 instance for a temporary job. Based on the input data, the job is most likely to finish within a week. Which of the following steps should be followed to terminate the instance automatically once the job is finished?

- A. Configure the EC2 instance with a stop instance to terminate it.
- B. Configure the EC2 instance with ELB to terminate the instance when it remains idle.
- C. Configure the CloudWatch alarm on the instance that should perform the termination action once the instance is idle.
- D. Configure the Auto Scaling schedule activity that terminates the instance after 7 days.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Auto Scaling can start and stop the instance at a pre-defined time. Here, the total running time is unknown. Thus, the user has to use the CloudWatch alarm, which monitors the CPU utilization. The user can create an alarm that is triggered when the average CPU utilization percentage has been lower than 10 percent for 24 hours, signaling that it is idle and no longer in use. When the utilization is below the threshold limit, it will terminate the instance as a part of the instance action.

Reference:

<http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html>

QUESTION 28 Which of the following is true of Amazon EC2 security group?

- A. You can modify the outbound rules for EC2-Classic.
- B. You can modify the rules for a security group only if the security group controls the traffic for just one instance.
- C. You can modify the rules for a security group only when a new instance is created.
- D. You can modify the rules for a security group at any time.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

Reference: <http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html>

QUESTION 29

An Elastic IP address (EIP) is a static IP address designed for dynamic cloud computing. With an EIP, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Your EIP is associated with your AWS account, not a particular EC2 instance, and it remains associated with your account until you choose to explicitly release it. By default how many EIPs is each AWS account limited to on a per region basis?

- A. 1
- B. 5
- C. Unlimited
- D. 10

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

By default, all AWS accounts are limited to 5 Elastic IP addresses per region for each AWS account, because public (IPv4) Internet addresses are a scarce public resource. AWS strongly encourages you to use an EIP primarily for load balancing use cases, and use DNS hostnames for all other inter-node communication.

If you feel your architecture warrants additional EIPs, you would need to complete the Amazon EC2 Elastic IP Address Request Form and give reasons as to your need for additional addresses. Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html#using-instance-addressing-limit>

QUESTION 30

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a

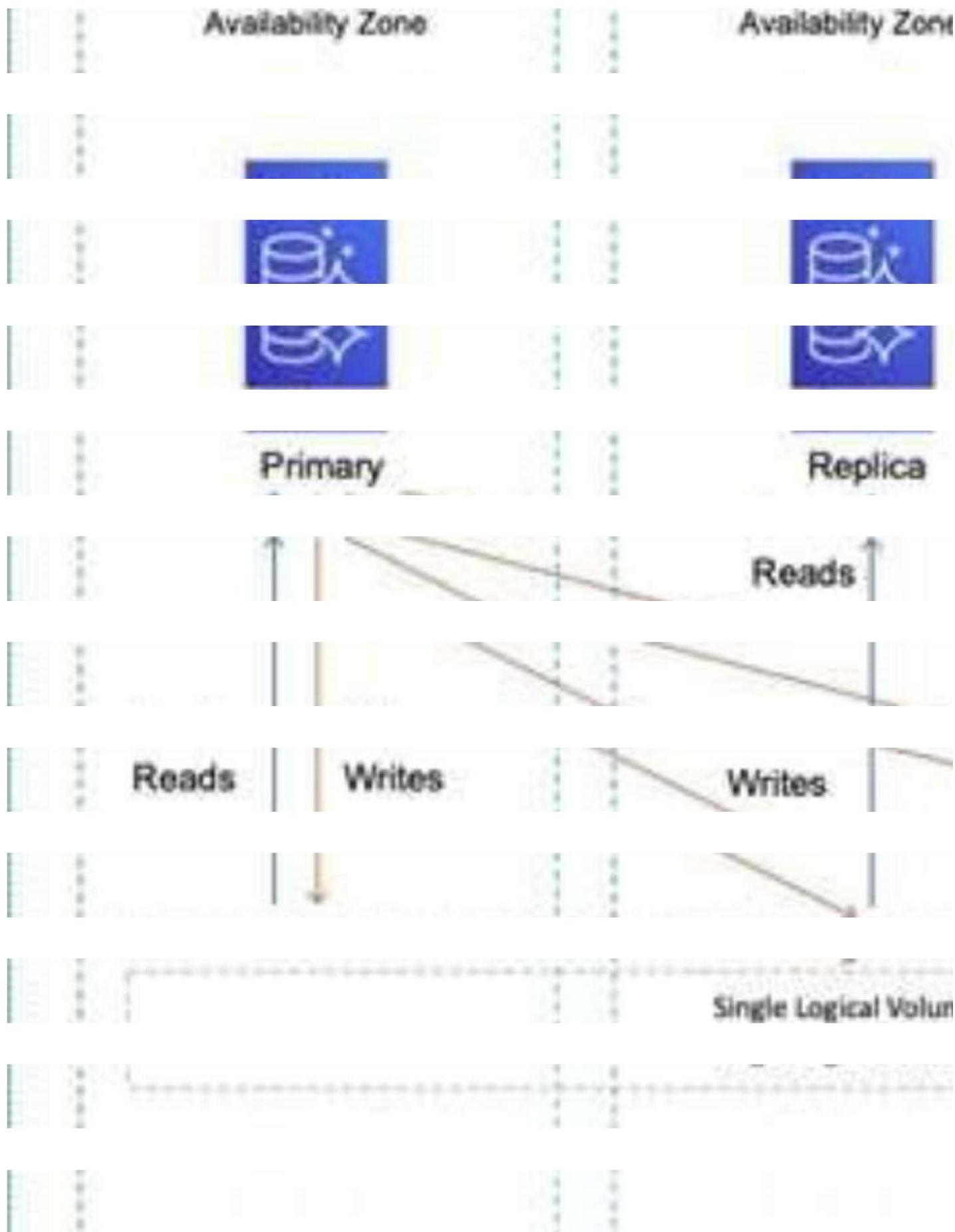


Region

DB cluster spans within an AWS Region. The DB cluster volume is made up of multiple copies of the data



for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster.



Data Copies

As well as providing scaling for reads, Aurora Replicas are also targets for multi-AZ. In this case the

Data Copies

solutions architect can update the application to read from the Multi-AZ standby instance.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

QUESTION 31

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to the changes in the metric due to a changing load pattern. CORRECT: "Use a target tracking policy to dynamically scale the Auto Scaling group" is the correct answer.

INCORRECT: "Use a simple scaling policy to dynamically scale the Auto Scaling group" is incorrect as target tracking is a better way to keep the aggregate CPU usage at around 40% INCORRECT: "Use an AWS Lambda function to update the desired Auto Scaling group capacity" is incorrect as this can be done automatically.

INCORRECT: "Use scheduled scaling actions to scale up and scale down the Auto Scaling group" is incorrect as dynamic scaling is required to respond to changes in utilization.

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

QUESTION 32

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database.

A solutions architect needs to make the application more resilient to periodic increases in request rates. Which architecture should the solutions architect implement? (Select TWO)

- A. Add AWS Shield.

- B. Add Aurora Replicas
- C. Add AWS Direct ConnectD. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation

The architecture is already highly resilient but the may be subject to performance degradation if there are sudden increases in request rates. To resolve this situation Amazon Aurora Read Replicas can be used to serve read traffic which offloads requests from the main database. On the frontend an Amazon CloudFront distribution can be placed in front of the ALB and this will cache content for better performance and also offloads requests from the backend.

CORRECT: "Add Amazon Aurora Replicas" is the correct answer. CORRECT: "Add an Amazon CloudFront distribution in front of the ALB" is the correct answer.

INCORRECT: "Add and Amazon WAF in front of the ALB" is incorrect. A web application firewall protects applications from malicious attacks. It does not improve performance. INCORRECT: "Add an Amazon Transit Gateway to the Availability Zones" is incorrect as this is used to connect on-premises networks to VPCs.

INCORRECT: "Add an Amazon Global Accelerator endpoint" is incorrect as this service is used for directing users to different instances of the application in different regions based on latency.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html> <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

QUESTION 33

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

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. Amazon Route 53
- D. Amazon S3 Transfer Acceleration

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon CloudFront can be used to stream video to users across the globe using a wide variety of protocols that are layered on top of HTTP. This can include both on-demand video as well as real time streaming video.

CORRECT: "Amazon CloudFront" is the correct answer.

INCORRECT: "AWS Global Accelerator" is incorrect as this would be an expensive way of getting the content closer to users compared to using CloudFront. As this is a use case for CloudFront and there are so many edge locations it is the better option. INCORRECT: "Amazon Route 53" is incorrect as you still need a solution for getting the content closer to users.

INCORRECT: "Amazon S3 Transfer Acceleration" is incorrect as this is used to accelerate uploads of data to Amazon S3 buckets.

References:

<https://aws.amazon.com/cloudfront/streaming/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html> **QUESTION 34**

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB).

Due to a recent change in copyright restrictions the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following:

Allow your users to access your content only if they're in one of the countries on a whitelist of approved countries.

Prevent your users from accessing your content if they're in one of the countries on a blacklist of banned countries.

For example, if a request comes from a country where, for copyright reasons, you are not authorized to distribute your content, you can use CloudFront geo restriction to block the request. This is the easiest and most effective way to implement a geographic restriction for the delivery of content.

CORRECT: "Use Amazon CloudFront to serve the application and deny access to blocked countries" is the correct answer.

INCORRECT: "Use a Network ACL to block the IP address ranges associated with the specific countries" is incorrect as this would be extremely difficult to manage. **INCORRECT:** "Modify the ALB security group to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.

INCORRECT: "Modify the security group for EC2 instances to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

QUESTION 35

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

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

Correct Answer: A

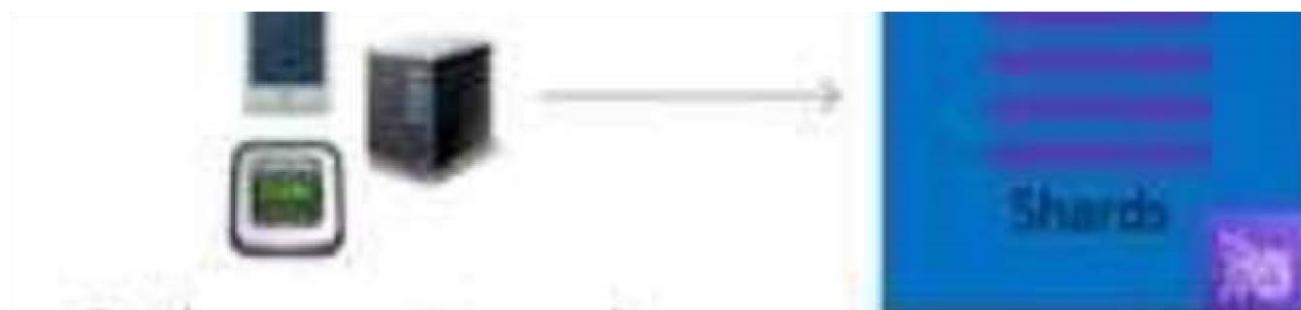
Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon Kinesis Data Streams collect and process data in real time. A Kinesis data stream is a set of



shards. Each shard has a sequence of data records. Each data record has a sequence number that is

assigned by Kinesis Data Streams. A shard is a uniquely identified sequence of data records in a stream. A partition key is used to group data by shard within a stream. Kinesis Data Streams segregates the data records belonging to a stream into multiple shards. It uses the partition key that is associated with each data record to determine which shard a given data record belongs to.

For this scenario, the solutions architect can use a partition key for each device. This will ensure the records for that device are grouped by shard and the shard will ensure ordering. Amazon S3 is a valid destination for saving the data records.

CORRECT: "Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3" is the correct answer. INCORRECT: "Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS" is incorrect as you cannot save data to EBS from Kinesis.

INCORRECT: "Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS" is incorrect as SQS is not the most efficient service for streaming, real time data. INCORRECT: "Use an Amazon SQS standard

queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3" is incorrect as SQS is not the most efficient service for streaming, real time data. References: <https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

QUESTION 36

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway.

When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal. Which combination of architectural changes will reduce the NAT gateway costs'? (Select TWO)

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture. <https://www.levvel.io/resource-library/aws-api-gateway-for-multi-account-architecture> There is no API listed in shareable resources for RAM.

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

QUESTION 37 In Amazon EC2, partial instance-hours are billed _____.

- A. per second used in the hour
- B. per minute used
- C. by combining partial segments into full hours
- D. as full hours

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Partial instance-hours are billed to the next hour.

Reference: <http://aws.amazon.com/ec2/faqs/>

QUESTION 38

In EC2, what happens to the data in an instance store if an instance reboots (either intentionally or unintentionally)?

- A. Data is deleted from the instance store for security reasons.
- B. Data persists in the instance store.
- C. Data is partially present in the instance store.

- D. Data in the instance store will be lost.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data on instance store volumes is lost under the following circumstances.

Failure of an underlying drive

Stopping an Amazon EBS-backed instance Terminating an instance Reference:

<http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/InstanceStorage.htm>

|

QUESTION 39

You are setting up a VPC and you need to set up a public subnet within that VPC. Which following requirement must be met for this subnet to be considered a public subnet?

- A. Subnet's traffic is not routed to an internet gateway but has its traffic routed to a virtual private gateway.
- B. Subnet's traffic is routed to an internet gateway.
- C. Subnet's traffic is not routed to an internet gateway.
- D. None of these answers can be considered a public subnet.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC: you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings. A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the Internet. If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet. If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway, the subnet is known as a VPN-only subnet.

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION 40

Can you specify the security group that you created for a VPC when you launch an instance in EC2Classic?

- A. No, you can specify the security group created for EC2-Classic when you launch a VPC instance.
- B. No
- C. Yes
- D. No, you can specify the security group created for EC2-Classic to a non-VPC based instance only.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If you're using EC2-Classic, you must use security groups created specifically for EC2-Classic. When you launch an instance in EC2-Classic, you must specify a security group in the same region as the instance. You can't specify a security group that you created for a VPC when you launch an instance in EC2-Classic.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#ec2-classic-securitygroups>

QUESTION 41

While using the EC2 GET requests as URLs, the _____ is the URL that serves as the entry point for the web service.

- A. token
- B. endpoint
- C. action
- D. None of these

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The endpoint is the URL that serves as the entry point for the web service. Reference: <http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-query-api.html>

QUESTION 42

You have been asked to build a database warehouse using Amazon Redshift. You know a little about it, including that it is a SQL data warehouse solution, and uses industry standard ODBC and JDBC connections and PostgreSQL drivers. However you are not sure about what sort of storage it uses for database tables. What sort of storage does Amazon Redshift use for database tables?

- A. InnoDB Tables
- B. NDB data storage
- C. Columnar data storage
- D. NDB CLUSTER Storage

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon Redshift achieves efficient storage and optimum query performance through a combination of massively parallel processing, columnar data storage, and very efficient, targeted data compression encoding schemes.

Columnar storage for database tables is an important factor in optimizing analytic query performance because it drastically reduces the overall disk I/O requirements and reduces the amount of data you need to load from disk.

Reference:

http://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmt.html

QUESTION 43

You are checking the workload on some of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes and it seems that the I/O latency is higher than you require. You should probably check the _____ to make sure that your application is not trying to drive more IOPS than you have provisioned.

- A. Amount of IOPS that are available

- B. Acknowledgement from the storage subsystem
- C. Average queue length
- D. Time it takes for the I/O operation to complete

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In EBS workload demand plays an important role in getting the most out of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes. In order for your volumes to deliver the amount of IOPS that are available, they need to have enough I/O requests sent to them. There is a relationship between the demand on the volumes, the amount of IOPS that are available to them, and the latency of the request (the amount of time it takes for the I/O operation to complete). Latency is the true end-to-end client time of an I/O operation; in other words, when the client sends a IO, how long does it take to get an acknowledgement from the storage subsystem that the IO read or write is complete.

If your I/O latency is higher than you require, check your average queue length to make sure that your application is not trying to drive more IOPS than you have provisioned. You can maintain high IOPS while keeping latency down by maintaining a low average queue length (which is achieved by provisioning more IOPS for your volume).

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-workload-demand.html>

QUESTION 44

Which of the below mentioned options is not available when an instance is launched by Auto Scaling with EC2 Classic?

- A. Public IP
- B. Elastic IP
- C. Private DNS
- D. Private IP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Auto Scaling supports both EC2 classic and EC2-VPC. When an instance is launched as a part of EC2 classic, it will have the public IP and DNS as well as the private IP and DNS.

Reference:

<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html>

QUESTION 45

You have been given a scope to deploy some AWS infrastructure for a large organisation. The requirements are that you will have a lot of EC2 instances but may need to add more when the average utilization of your Amazon EC2 fleet is high and conversely remove them when CPU utilization is low. Which AWS services would be best to use to accomplish this?

- A. Auto Scaling, Amazon CloudWatch and AWS Elastic Beanstalk
- B. Auto Scaling, Amazon CloudWatch and Elastic Load Balancing.
- C. Amazon CloudFront, Amazon CloudWatch and Elastic Load Balancing.
- D. AWS Elastic Beanstalk , Amazon CloudWatch and Elastic Load Balancing.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Auto Scaling enables you to follow the demand curve for your applications closely, reducing the need to manually provision Amazon EC2 capacity in advance. For example, you can set a condition to add new Amazon EC2 instances in increments to the Auto Scaling group when the average utilization of your Amazon EC2 fleet is high; and similarly, you can set a condition to remove instances in the same increments when CPU utilization is low. If you have predictable load changes, you can set a schedule through Auto Scaling to plan your scaling activities. You can use Amazon CloudWatch to send alarms to trigger scaling activities and Elastic Load Balancing to help distribute traffic to your instances within Auto Scaling groups. Auto Scaling enables you to run your Amazon EC2 fleet at optimal utilization.

Reference: <http://aws.amazon.com/autoscaling/>

QUESTION 46

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption.

Due to new compliance requirements, all existing and new data in this database must be encrypted.

How should this be accomplished?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 47**

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

Which solution meets these requirements'?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation

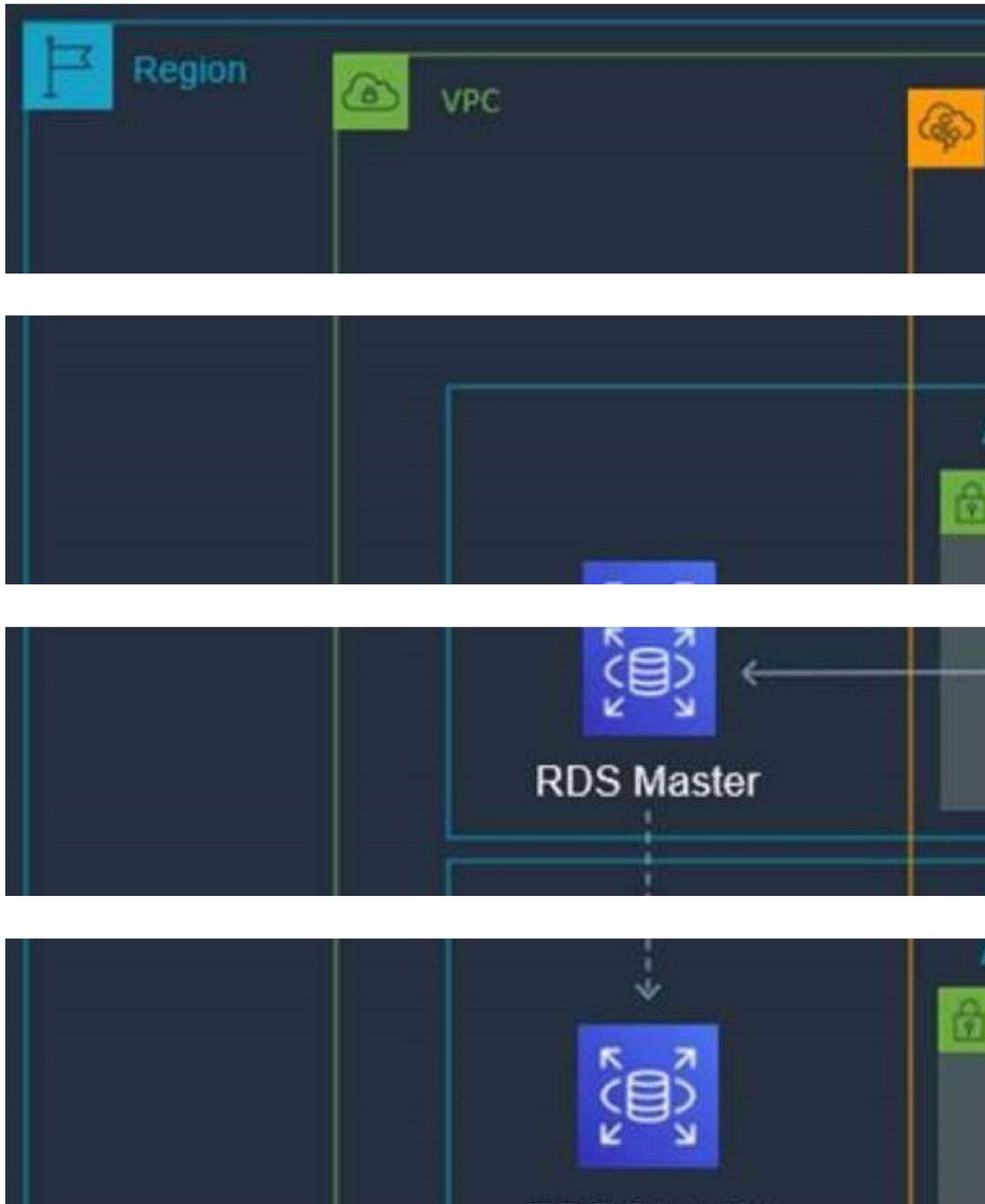
Keyword: Highly available + Least amount of changes to the application High Availability = Multi-AZ

Least amount of changes to the application = Elastic Beanstalk Automatically handles the

deployment, from Capacity provisioning, Load Balancing, Auto Scaling to application health monitoring

Option - D will be the right choice and Option - A; Option - B and Option - C out of race due to Cost & interoperability.

HA with Elastic Beanstalk and RDS



RDS Standby

AWS Elastic Beanstalk

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

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

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

AWS RDS

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating timeconsuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

Amazon RDS is available on several database instance types - optimized for memory, performance or I/O and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. You can use the AWS Database Migration Service to easily migrate or replicate your existing databases to Amazon RDS.

AWS S3

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finelytuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.99999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

References:

https://aws.amazon.com/elasticbeanstalk/?nc2=h_ql_prod_cp_ebs https://aws.amazon.com/rds/?nc2=h_ql_prod_db_rds
https://aws.amazon.com/s3/?nc2=h_ql_prod_st_s3

QUESTION 48

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer.

The web server is vulnerable to cross-site scripting (XSS) attacks. What should a solutions architect do to remediate the vulnerability?

- A. Create a Classic Load Balancer.
Put the web layer behind the load balancer and enable AWS WAF.
- B. Create a Network Load Balancer.

- Put the web layer behind the load balancer and enable AWS WAF.
- C. Create an Application Load Balancer.
Put the web layer behind the load balancer and enable AWS WAF.
- D. Create an Application Load Balancer.
Put the web layer behind the load balancer and use AWS Shield Standard.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The AWS Web Application Firewall (WAF) is available on the Application Load Balancer (ALB). You can use AWS WAF directly on Application Load Balancers (both internal and external) in a VPC, to protect your websites and web services.

Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF to inspect for possible malicious scripts.

CORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is the correct answer.

INCORRECT: "Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a classic load balancer. **INCORRECT:** "Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a network load balancer. **INCORRECT:** "Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard" is incorrect as you cannot use AWS Shield to protect against XSS attacks. Shield is used to protect against DDoS attacks.

References: <https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html>

QUESTION 49

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month.

Each application has approximately 50 TB of data to be transferred. After the migration is complete this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity.

Which solution will meet these requirements"

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Each application has approximately 50 TB of data to be transferred" = AWS Snowball; "secure network connectivity with consistent throughput from their data centers to the applications" What are the benefits of using AWS Direct Connect and private network connections? In many circumstances, private network connections can reduce costs, increase bandwidth, and provide a more consistent network experience than Internet-based connections. "more consistent network experience", hence AWS Direct Connect. Direct Connect is better than VPN; reduced cost+increased bandwidth+(remain connection or consistent network) = direct connect

QUESTION 50

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket.

A solutions architect has been asked to design an efficient and effective solution. Which action should the solutions architect take to accomplish this?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon CloudFront can be used to cache the files in edge locations around the world and this will improve the performance of the webpages.

To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:

Using a REST API endpoint as the origin with access restricted by an origin access identity (OAI) Using a website endpoint as the origin with anonymous (public) access allowed Using a website endpoint as the origin with access restricted by a Referer header **CORRECT**:

"Use Amazon CloudFront with the S3 bucket as its origin" is the correct answer. **INCORRECT**: "Generate presigned URLs for the files" is incorrect as this is used to restrict access which is not a requirement.

INCORRECT: "Use cross-Region replication to all Regions" is incorrect as this does not provide a mechanism for directing users to the closest copy of the static webpages. **INCORRECT**: "Use the geoproximity feature of Amazon Route 53" is incorrect as this does not include a solution for having multiple copies of the data in different geographic locations.

References: <https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

QUESTION 51

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently.

Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The application is writing the files using API calls which means it will be compatible with Amazon S3 which uses a REST API. S3 is a massively scalable key-based object store that is well-suited to allowing concurrent access to the files from many instances. Amazon S3 will also be the most cost-effective choice. A rough calculation using the AWS pricing calculator shows the cost differences between 1TB of storage on EBS, EFS, and S3 Standard.

Amazon Elastic Block Store (EBS) Region: US East (Ohio)	<input type="button" value="Edit"/> <input type="button" value="Action"/>
Amazon Elastic Block Storage (EBS) Number of instances (1), Average duration each instance runs (730 hours per month), Storage amount (1 TB), Snapshot Frequency (2x Daily), Amount charged per snapshot (3 GB).	Monthly \$16.09 USD
Amazon Elastic File System (EFS) Region: US East (Ohio)	<input type="button" value="Edit"/> <input type="button" value="Action"/>
Data stored in Standard storage (1 TB per month)	Monthly \$07.29 USD
Amazon Simple Storage Service (S3)	<input type="button" value="Edit"/> <input type="button" value="Action"/>
S3 Standard storage (1 TB per month)	Monthly \$4.41 USD

CORRECT: "Amazon S3" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as though this does offer concurrent access from many EC2 Linux instances, it is not the most cost-effective solution. INCORRECT: "Amazon EBS" is incorrect. The Elastic Block Store (EBS) is not a good solution for concurrent access from many EC2 instances and is not the most cost-effective option either. EBS volumes are mounted to a single instance except when using multi-attach which is a new feature and has several constraints.

INCORRECT: "Amazon EC2 instance store" is incorrect as this is an ephemeral storage solution which means the data is lost when powered down.

Therefore, this is not an option for long-term data storage.

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

QUESTION 52

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

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

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0

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

from the security group for the web tier

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Inbound: Protocol/Port HT

Explanation:

Outbound: Protocol/Port HT

In this scenario an inbound rule is required to allow traffic from any internet client to the web front end on

SSL/TLS port 443. The source should therefore be set to 0.0.0.0/0 to allow any inbound traffic.

To secure the connection from the web frontend to the database tier, an outbound rule should be created

from the public EC2 security group with a destination of the private EC2 security group. The port should be

set to 1433 for MySQL. The private EC2 security group will also need to allow inbound traffic on 1433 from the public EC2 security group.

This configuration can be seen in the diagram:

Private subnet(s)

Inbound: Protocol/Port HTTP

CORRECT: "Configure the security group for the web tier to allow inbound traffic on port 443 from

0.0.0.0/0" is a correct answer.

CORRECT: "Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier" is also a correct answer. INCORRECT: "Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0" is incorrect as this is configured backwards. INCORRECT: "Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier" is incorrect as the MySQL database instance does not need to send outbound traffic on either of these ports. INCORRECT: "Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier" is incorrect as the database tier does not need to allow inbound traffic on port 443.

References:

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

QUESTION 54

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object. CORRECT: "Amazon S3 Standard" is the correct answer.

INCORRECT: "Amazon S3 Intelligent-Tiering" is incorrect as there is an additional fee for using this service and for a short-term requirement it may not be beneficial. INCORRECT: "Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as this storage class has a minimum capacity charge per object (128 KB) and a per GB retrieval fee. INCORRECT: "Amazon S3 Glacier Deep Archive" is incorrect as this storage class is used for archiving data. There are retrieval fees and it takes hours to retrieve data from an archive. References: <https://aws.amazon.com/s3/storage-classes/>

QUESTION 55

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores useruploaded documents in an Amazon EBS volume.

For better scalability and availability the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone: placing both behind an Application Load Balancer. After completing this change users reported that each time they refreshed the website they could see one subset of their documents or the other but never all of the documents at the same time. What should a solutions architect propose to ensure users see all of their documents at once"

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents.
- C. Copy the data from both EBS volumes to Amazon EFS.

- Modify the application to save new documents to Amazon EPS.
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

You are building infrastructure for a data warehousing solution and an extra request has come through that there will be a lot of business reporting queries running all the time and you are not sure if your current DB instance will be able to handle it. What would be the best solution for this?

- A. DB Parameter Groups
- B. Read Replicas
- C. Multi-AZ DB Instance deployment
- D. Database Snapshots

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Read Replicas make it easy to take advantage of MySQL's built-in replication functionality to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. There are a variety of scenarios where deploying one or more Read Replicas for a given source DB Instance may make sense. Common reasons for deploying a Read Replica include:

Scaling beyond the compute or I/O capacity of a single DB Instance for read-heavy database workloads. This excess read traffic can be directed to one or more Read Replicas. Serving read traffic while the source DB Instance is unavailable. If your source DB Instance cannot take I/O requests (e.g. due to I/O suspension for backups or scheduled maintenance), you can direct read traffic to your Read Replica(s). For this use case, keep in mind that the data on the Read Replica may be "stale" since the source DB Instance is unavailable. Business reporting or data warehousing scenarios; you may want business reporting queries to run against a Read Replica, rather than your primary, production DB Instance.

Reference: <https://aws.amazon.com/rds/faqs/>

QUESTION 57

In DynamoDB, could you use IAM to grant access to Amazon DynamoDB resources and API actions?

- A. In DynamoDB there is no need to grant access
- B. Depended to the type of access
- C. No
- D. Yes

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon DynamoDB integrates with AWS Identity and Access Management (IAM). You can use AWS IAM to grant access to Amazon DynamoDB resources and API actions. To do this, you first write an AWS IAM policy, which is a document that explicitly lists the permissions you want to grant. You then attach that policy to an AWS IAM user or role.

Reference:

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/UsingIAMWithDDB.html>

Exam C

QUESTION 1

Much of your company's data does not need to be accessed often, and can take several hours for retrieval time, so it's stored on Amazon Glacier. However someone within your organization has expressed concerns that his data is more sensitive than the other data, and is wondering whether the high level of encryption that he knows is on S3 is also used on the much cheaper Glacier service. Which of the following statements would be most applicable in regards to this concern?

- A. There is no encryption on Amazon Glacier, that's why it is cheaper.
- B. Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method thanAmazon S3 but you can change it to AES-256 if you are willing to pay more.
- C. Amazon Glacier automatically encrypts the data using AES-256, the same as Amazon S3.
- D. Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method thanAmazon S3.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Like Amazon S3, the Amazon Glacier service provides low-cost, secure, and durable storage. But where S3 is designed for rapid retrieval, Glacier is meant to be used as an archival service for data that is not accessed often, and for which retrieval times of several hours are suitable. Amazon Glacier automatically encrypts the data using AES-256 and stores it durably in an immutable form. Amazon Glacier is designed to provide average annual durability of 99.99999999% for an archive. It stores each archive in multiple facilities and multiple devices. Unlike traditional systems which can require laborious data verification and manual repair, Glacier performs regular, systematic data integrity checks, and is built to be automatically self-healing. Reference:

<http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf>

QUESTION 2

Your EBS volumes do not seem to be performing as expected and your team leader has requested you look into improving their performance. Which of the following is not a true statement relating to the performance of your EBS volumes?

- A. Frequent snapshots provide a higher level of data durability and they will not degrade the performanceof your application while the snapshot is in progress.
- B. General Purpose (SSD) and Provisioned IOPS (SSD) volumes have a throughput limit of 128 MB/s pervolume.
- C. There is a relationship between the maximum performance of your EBS volumes, the amount of I/O youare driving to them, and the amount of time it takes for each transaction to complete.
- D. There is a 5 to 50 percent reduction in IOPS when you first access each block of data on a newlycreated or restored EBS volume

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Several factors can affect the performance of Amazon EBS volumes, such as instance configuration, I/O characteristics, workload demand, and storage configuration. Frequent snapshots provide a higher level of data durability, but they may slightly degrade the performance of your application while the snapshot is in

progress. This trade off becomes critical when you have data that changes rapidly. Whenever possible, plan for snapshots to occur during off-peak times in order to minimize workload impact.

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html>

QUESTION 3

You've created your first load balancer and have registered your EC2 instances with the load balancer. Elastic Load Balancing routinely performs health checks on all the registered EC2 instances and automatically distributes all incoming requests to the DNS name of your load balancer across your registered, healthy EC2 instances. By default, the load balancer uses the ___ protocol for checking the health of your instances.

- A. HTTPS
- B. HTTP
- C. ICMP
- D. IPv6

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In Elastic Load Balancing a health configuration uses information such as protocol, ping port, ping path (URL), response timeout period, and health check interval to determine the health state of the instances registered with the load balancer.

Currently, HTTP on port 80 is the default health check.

Reference:

<http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyConcepts.html>

QUESTION 4

A major finance organisation has engaged your company to set up a large data mining application. Using AWS you decide the best service for this is Amazon Elastic MapReduce(EMR) which you know uses Hadoop. Which of the following statements best describes Hadoop?

- A. Hadoop is 3rd Party software which can be installed using AMI
- B. Hadoop is an open source python web framework
- C. Hadoop is an open source Java software framework
- D. Hadoop is an open source javascript framework

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon EMR uses Apache Hadoop as its distributed data processing engine. Hadoop is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware. Hadoop implements a programming model named "MapReduce," where the data is divided into many small fragments of work, each of which may be executed on any node in the cluster. This framework has been widely used by developers, enterprises and startups and has proven to be a reliable software platform for processing up to petabytes of data on clusters of thousands of commodity machines.

Reference: <http://aws.amazon.com/elasticmapreduce/faqs/>

QUESTION 5 In Amazon EC2 Container Service, are other container types supported?

- A. Yes, EC2 Container Service supports any container service you need.
- B. Yes, EC2 Container Service also supports Microsoft container service.
- C. No, Docker is the only container platform supported by EC2 Container Service presently.
- D. Yes, EC2 Container Service supports Microsoft container service and Openstack.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In Amazon EC2 Container Service, Docker is the only container platform supported by EC2 Container Service presently.

Reference: <http://aws.amazon.com/ecs/faqs/>

QUESTION 6

A Solutions Architect is designing the architecture for a web application that will be hosted on AWS. Internet users will access the application using HTTP and HTTPS.

How should the Architect design the traffic control requirements?

- A. Use a network ACL to allow outbound ports for HTTP and HTTPS. Deny other traffic for inbound and outbound.
- B. Use a network ACL to allow inbound ports for HTTP and HTTPS. Deny other traffic for inbound and outbound.
- C. Allow inbound ports for HTTP and HTTPS in the security group used by the web servers.
- D. Allow outbound ports for HTTP and HTTPS in the security group used by the web servers.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed.

The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started.

Once completed, the system is expected to run for a minimum of 1 year. Which type of Amazon EC2 instances should be used to reduce the cost of the system?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week. CORRECT: "Scheduled Reserved Instances" is the correct answer. INCORRECT: "Standard Reserved Instances" is incorrect as the workload only runs for 4 hours a day this would be more expensive.

INCORRECT: "On-Demand Instances" is incorrect as this would be much more expensive as there is no discount applied.

INCORRECT: "Spot Instances" is incorrect as the workload cannot be interrupted once started. With Spot instances workloads can be terminated if the Spot price changes or capacity is required.

References: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

QUESTION 8

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The most cost-effective option is to migrate the website to an Amazon S3 bucket and configure that bucket for static website hosting. To enable good performance for global users the solutions architect should then configure a CloudFront distribution with the S3 bucket as the origin. This will cache the static content around the world closer to users. CORRECT: "Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin" is the correct answer.

INCORRECT: "Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions" is incorrect as there is no solution here for directing users to the closest region. This could be a more cost-effective (though less elegant) solution if AWS Route 53 latency records are created. INCORRECT: "Copy the website content to an Amazon EC2 instance. Configure Amazon Route 53 geolocation routing policies to select the closest origin" is incorrect as using Amazon EC2 instances is less cost-effective compared to hosting the website on S3.

Also, geolocation routing does not achieve anything with only a single record.

INCORRECT: "Copy the website content to multiple Amazon EC2 instances in multiple AWS Regions. Configure AWS Route 53 geolocation routing policies to select the closest region" is incorrect as using Amazon EC2 instances is less cost-effective compared to hosting the website on S3.

References: <https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

QUESTION 9

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage.

The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available.

Users must be able to download, modify, and upload documents. Which combination of actions should be taken to meet these requirements? (Select TWO)

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

None of the options present a good solution for specifying permissions required to write and modify objects so that requirement needs to be taken care of separately. The other requirements are to prevent accidental deletion and ensure that all versions of the document are available. The two solutions for these requirements are versioning and MFA delete. Versioning will retain a copy of each version of the document and multi-factor authentication delete (MFA delete) will prevent any accidental deletion as you need to supply a second factor when attempting a delete. CORRECT: "Enable versioning on the bucket" is a correct answer. CORRECT: "Enable MFA Delete on the bucket" is also a correct answer. INCORRECT: "Set readonly permissions on the bucket" is incorrect as this will also prevent any writing to the bucket which is not desired. INCORRECT: "Attach an IAM policy to the bucket" is incorrect as users need to modify documents which will also allow delete. Therefore, a method must be implemented to just control deletes.

INCORRECT: "Encrypt the bucket using AWS SSE-S3" is incorrect as encryption doesn't stop you from deleting an object.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html> <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

QUESTION 10

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance.

The backend application then stores the data in Amazon RDS. What should a solutions architect do to decouple the architecture and make it scalable?"

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation

Keyword: Static + Decouple + Scalable

Static=S3

Decouple=SQS Queue

Scalable=ASG

Option B will not be there in the race due to Auto-Scaling unavailability. Option A will not be there in the race due to Decouple unavailability. Option C & D will be in the race and Option D will be correct answers due to all 3 combination matches [Static=S3; Decouple=SQS Queue; Scalable=ASG] & Option C will loose due to Static option unavailability

QUESTION 11

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

Which of the following would be the LEAST complicated implementation?

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

Correct Answer: C**Section: (none)**

Explanation

Explanation/Reference:**QUESTION 12**

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

What should a solutions architect do to accomplish this?

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

Correct Answer: A**Section: (none)**

Explanation

Explanation/Reference:

Explanation:

The maximum size of a single file that can be delivered through Amazon CloudFront is 20 GB. This limit applies to all Amazon CloudFront distributions.

QUESTION 13

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

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

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

[https://d0.awsstatic.com/whitepapers/whitepaper-streaming-data-solutions-on-aws-with-amazonkinesis.pdf \(9\)](https://d0.awsstatic.com/whitepapers/whitepaper-streaming-data-solutions-on-aws-with-amazonkinesis.pdf)

https://aws.amazon.com/kinesis/#Evolve_from_batch_to_real-time_analytics

QUESTION 14

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries.

These performance issues were caused by users generating different real-time reports from the application during working hours.

Which solution will improve the performance of the application when it is moved to AWS?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The MySQL-compatible edition of Aurora delivers up to 5X the throughput of standard MySQL running on the same hardware, and enables existing MySQL applications and tools to run without requiring modification. <https://aws.amazon.com/rds/aurora/mysql-features/>

QUESTION 15

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

What should a solutions architect do to accomplish this?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"ELB provides load balancing within one Region, AWS Global Accelerator provides traffic management across multiple Regions [...] AWS Global Accelerator complements ELB by extending these capabilities beyond a single AWS Region, allowing you to provision a global interface for your applications in any number of Regions. If you have workloads that cater to a global client base, we recommend that you use AWS Global Accelerator. If you have workloads hosted in a single AWS Region and used by clients in and around the same Region, you can use an Application Load Balancer or Network Load Balancer to manage your resources." <https://aws.amazon.com/global-accelerator/faqs/>

QUESTION 16

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

How should a solutions architect design the S3 solution?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region. Both source and destination buckets must have versioning enabled. CORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-Region replication" is the correct answer.

INCORRECT: "Create an additional S3 bucket in another Region and configure cross-Region replication" is incorrect as the destination bucket must also have versioning enabled. INCORRECT: "Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication. INCORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication.

References:

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

QUESTION 17

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Gateway Endpoint for S3 and DynamoDB

<https://medium.com/tensult/aws-vpc-endpoints-introduction-ef2bf85c4422> <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpcgateway.html>

QUESTION 18

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month. Accountants run large queries that impact the database's performance due to high usage.

The company wants to minimize the impact that the reporting activity has on the web application. What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon RDS uses the MariaDB, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server DB engines' built-in replication functionality to create a special type of DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica.

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

QUESTION 19

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted.

The company wants to minimize costs.

Which pricing model should the company choose?

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

D. Scheduled Reserved Instances

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

QUESTION 20

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

Which configuration should the solutions architect choose to meet these requirements?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

(geolocation routing) QUESTION 21

A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage.

There are other internal systems that query this DB instance to fetch data for internal batch processing.

The RDS DB instance slows down significantly the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times. Which solution will improve the website's performance?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux.

The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.

Which storage option would be the optimal solution?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

https://d1.awsstatic.com/whitepapers/AWS%20Partner%20Network_HPC%20Storage%20Options_2019_FINAL.pdf (p.8)

QUESTION 23

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS.

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Migrate AD to AWS Managed AD and keep the webserver alone.. Reduce risk = remove AD from that EC2.

Minimize admin = remove AD from any EC2

-> use AWS Directory Service

Active Directory connector is only for ON-PREM AD. The one they have exists in the cloud already.

QUESTION 24

A company runs an application in a branch office within a small data closet with no virtualized compute resources.

The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meets these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation

Keyword: NFS + Compliance

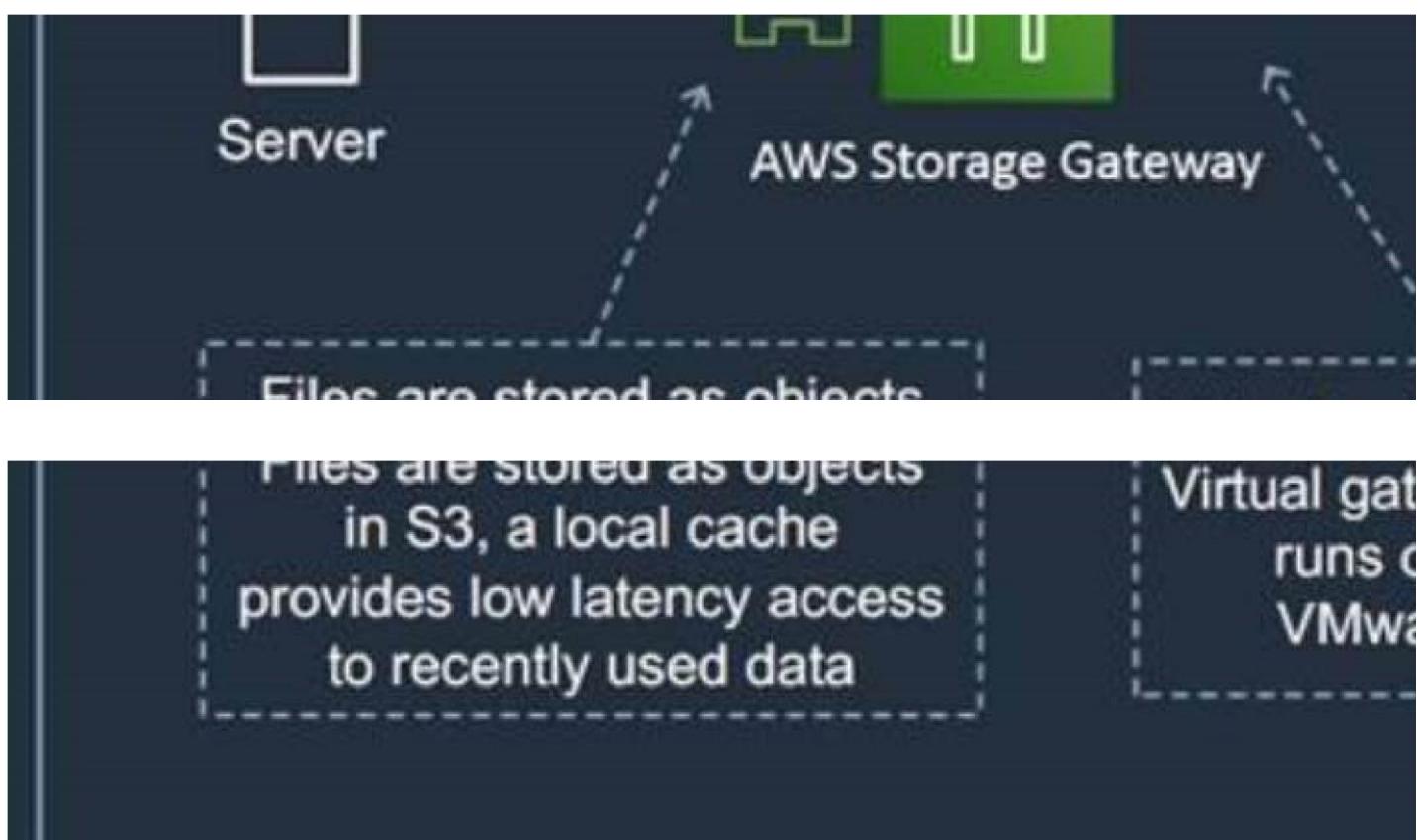
File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2- resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.

AWS Storage Gateway File Gateway



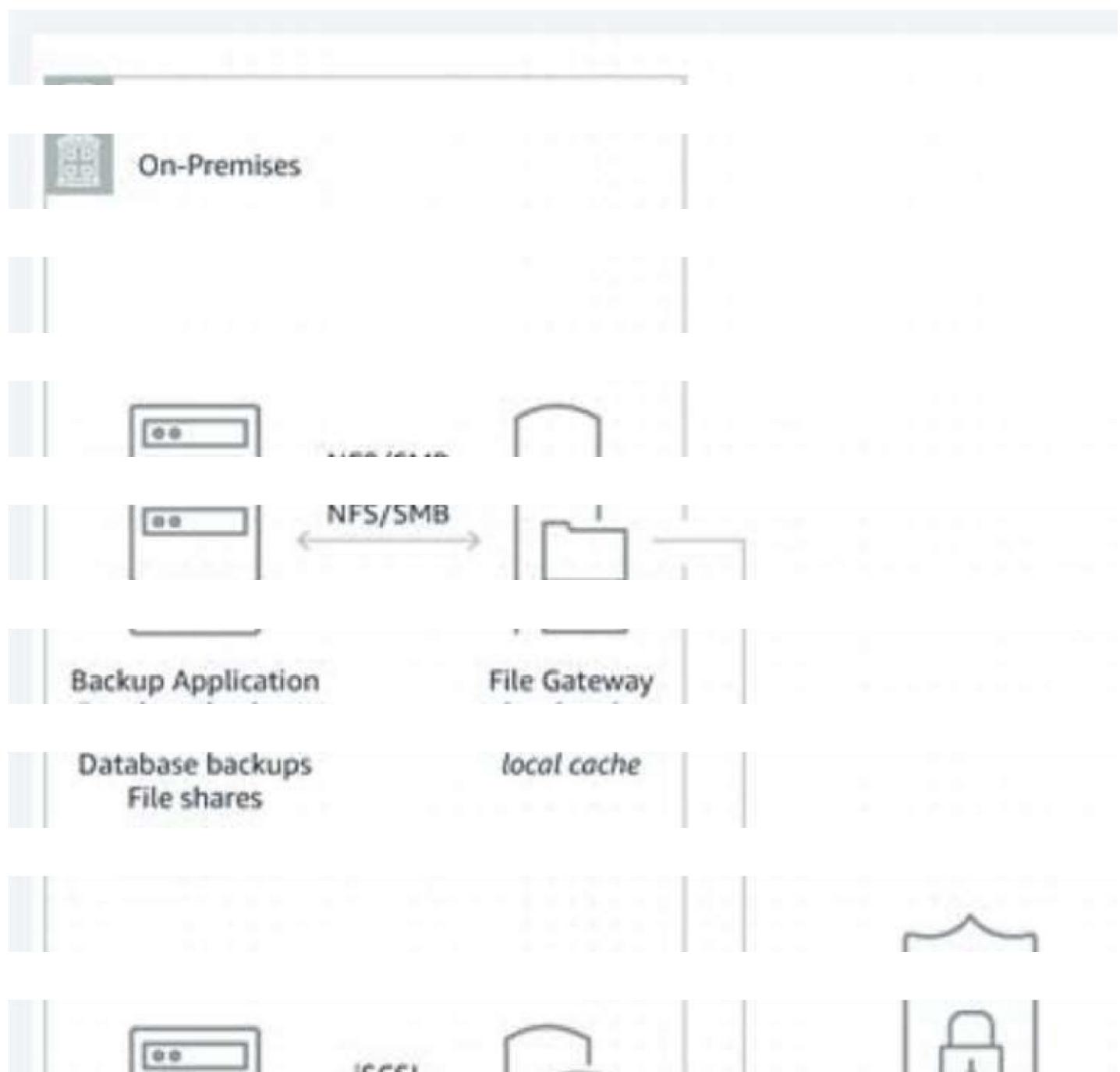


The table below shows the different gateways available and the interfaces and use cases:



New Name	Old Name	Interface	Use Case
File Gateway	None	NFS, SMB	Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount point

Volume Gateway Stored Mode	Gateway-Stored Volumes	iSCSI	Asynchronous replication of on-prem data to S3
Volume Gateway Cached Mode	Gateway-Cached Volumes	iSCSI	Primary data stored in S3 with frequently accessed data cached locally on-prem
Storage Gateway Overview			
Tape Gateway	Gateway-Virtual Tape Library	iSCSI	Virtual media changer and tape library for use with existing backup software



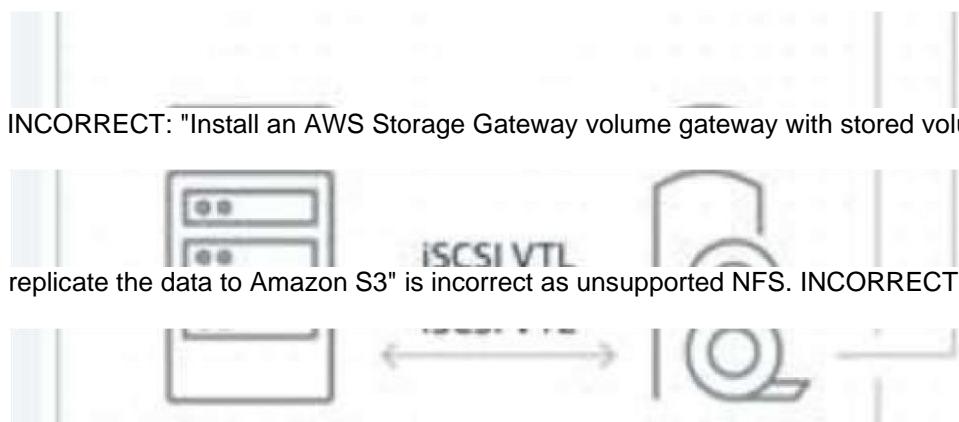
CORRECT: "Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3" is the correct answer.



the data to Amazon S3" is the correct answer.

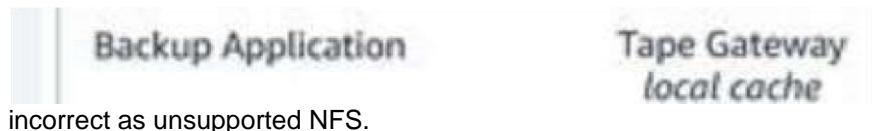


S3" is incorrect.



INCORRECT: "Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3" is incorrect as unsupported NFS. INCORRECT: "Install an AWS Storage

Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3" is



incorrect as unsupported NFS.

References:

<https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/> <https://d0.awsstatic.com/>

whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf

QUESTION 25

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size.

The application owner will make the log file available to the vendor for a limited time. What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor.

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an Auto Scaling group.

The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate.

The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website. What should a solutions architect do to meet these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table.

What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation

VPC Endpoint

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.

AWS PrivateLink access over Inter-Region VPC Peering:

Applications in an AWS VPC can securely access AWS PrivateLink endpoints across AWS

■

Regions using Inter-Region VPC Peering.

AWS PrivateLink allows you to privately access services hosted on AWS in a highly available

■

and scalable manner, without using public IPs, and without requiring the traffic to traverse the Internet. Customers can privately connect to a service even if the service endpoint resides in a different

AWS Region.

Traffic using Inter-Region VPC Peering stays on the global AWS backbone and never traverses

the public Internet.

A gateway endpoint is a gateway that is a target for a specified route in your route table, used

for traffic destined to a supported AWS service.

An interface VPC endpoint (interface endpoint) enables you to connect to services powered by

AWS PrivateLink.

The table below highlights some key information about both types of endpoint:

References: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

QUESTION 31

A solutions architect needs to design a low-latency solution for a static single-page application accessed by users utilizing a custom domain name. The solution must be serverless, encrypted in transit, and costeffective.

Which combination of AWS services and features should the solutions architect use? (Select TWO.)

- A. Amazon S3
- B. Amazon EC2

- C. AWS Fargate

- D. Amazon CloudFront
- E. Elastic Load Balancer

What

Elastic Netw

How

Uses DNS en

Which services

API Gateway

CloudWatch

Correct Answer: AD

Security

Security Group

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

A company has global users accessing an application deployed in different AWS Regions, exposing public static IP addresses. The users are experiencing poor performance when accessing the application over the internet.

What should a solutions architect recommend to reduce internet latency?

- A. Set up AWS Global Accelerator and add endpoints.
- B. Set up AWS Direct Connect locations in multiple Regions.
- C. Set up an Amazon CloudFront distribution to access an application.
- D. Set up an Amazon Route 53 geoproximity routing policy to route traffic.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AWS Global Accelerator is a service in which you create accelerators to improve availability and performance of your applications for local and global users. Global Accelerator directs traffic to optimal endpoints over the AWS global network. This improves the availability and performance of your internet applications that are used by a global audience. Global Accelerator is a global service that supports endpoints in multiple AWS Regions, which are listed in the AWS Region Table. By default, Global Accelerator provides you with two static IP addresses that you associate with your accelerator. (Or, instead of using the IP addresses that Global Accelerator provides, you can configure these entry points to be IPv4 addresses from your own IP address ranges that you bring to Global Accelerator.)

Edge location

Resolve [detlahs.com](#)



Answer

Answer

51.45.2.12

Amazon

53.58.31.89

The static IP addresses are anycast from the AWS edge network and distribute incoming application traffic

across multiple endpoint resources in multiple AWS Regions, which increases the availability of your applications. Endpoints can be Network Load Balancers, Application Load Balancers, EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.

CORRECT: "Set up AWS Global Accelerator and add endpoints" is the correct answer. INCORRECT: "Set up AWS Direct Connect locations in multiple Regions" is incorrect as this is used to connect from an on-premises data center to AWS. It does not improve performance for users who are not connected to the on-premises data center. INCORRECT: "Set up an Amazon CloudFront distribution to access an application" is incorrect as CloudFront cannot expose static public IP addresses.

INCORRECT: "Set up an Amazon Route 53 geoproximity routing policy to route traffic" is incorrect as this does not reduce internet latency as well as using Global Accelerator. GA will direct users to the closest edge location and then use the AWS global network.

References: <https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

QUESTION 33

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

A solutions architect is designing a customer-facing application. The application is expected to have a

variable amount of reads and writes depending on the time of year and clearly defined access patterns throughout the year. Management requires that database auditing and scaling be managed in the AWS Cloud. The Recovery Point Objective (RPO) must be less than 5 hours. Which solutions can accomplish this? (Select TWO.)

- A. Use Amazon DynamoDB with auto scaling.
 Use on-demand backups and AWS CloudTrail.
- B. Use Amazon DynamoDB with auto scaling.
 Use on-demand backups and Amazon DynamoDB Streams.
- C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging.
 Perform database snapshots every 4 hours.
- D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter.
 Perform database snapshots every 5 hours.
- E. Use Amazon RDS with auto scaling.
 Enable the database auditing parameter.
 Configure the backup retention period to at least 1 day.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail. CORRECT Scalable, with backup and AWS Managed Auditing B. Use Amazon DynamoDB with auto scaling. Use ondemand backups and Amazon DynamoDB Streams.

INCORRECT - AWS DDB Streams can be used for auditing, but its not AWS managed auditing. C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.

INCORRECT - Not a database. Datalake

D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform databasesnapshots every 5 hours. INCORRECT - This does not scale

E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backupretention period to at least 1 day.

CORRECT - Scalable, AWS managed auditing and backup. The backup frequency is not stated but have no technical limitation which states it cannot be less 5 hours (1 day is retention period of the backup).

QUESTION 35

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A textbook case for CloudFront. The data transfer cost in CloudFront is lower than in S3. With heavy read operations of static content, it's more economical to add CloudFront in front of you S3 bucket.

QUESTION 36

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

Policy1

```
{  
    "Version": "2012-10-17", "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iam:Get*",  
                "iam>List*",
```

```

        "kms>List*",
        "ec2:*",
        "ds:*",
        "logs:Get*",
        "logs:Describe*"
    ],
    "Resource": "*"
}
1
}

}

```

Policy2

```

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

```

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

A solutions architect is helping a developer design a new ecommerce shopping cart application using AWS services. The developer is unsure of the current database schema and expects to make changes as the ecommerce site grows. The solution needs to be highly resilient and capable of automatically scaling read and write capacity.

Which database solution meets these requirements?

- A. Amazon Aurora PostgreSQL
- B. Amazon DynamoDB with on-demand enabled
- C. Amazon DynamoDB with DynamoDB Streams enabled
- D. Amazon SQS and Amazon Aurora PostgreSQL

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: <https://aws.amazon.com/pt/about-aws/whats-new/2018/11/announcing-amazon-dynamodb-on-demand/>

QUESTION 38

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications. Which solution will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

A solutions architect is designing a mission-critical web application. It will consist of Amazon EC2 instances behind an Application Load Balancer and a relational database. The database should be highly available and fault tolerant.

Which database implementations will meet these requirements? (Select TWO.)

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

Correct Answer: DE

Section: (none)**Explanation****Explanation/Reference:****QUESTION 41**

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

- A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
- B. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage
- C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage
- D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Correct Answer: A**Section: (none)****Explanation****Explanation/Reference:****QUESTION 42**

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

Which solution should the solutions architect recommend?

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

Correct Answer: B**Section: (none)****Explanation****Explanation/Reference:****Explanation:**

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time.

Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

In this case the volume would have a baseline performance of $3 \times 200 = 600$ IOPS. The volume could also burst to 3,000 IOPS for extended periods. As the I/O varies, this should be suitable. CORRECT: "Amazon EBS General Purpose SSD (gp2)" is the correct answer. INCORRECT: "Amazon EBS Provisioned IOPS

SSD (io1) " is incorrect as this would be a more expensive option and is not required for the performance characteristics of this workload. INCORRECT: "Amazon EBS Cold HDD (sc1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload. INCORRECT: "Amazon EBS Throughput Optimized HDD (st1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload. References:
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

QUESTION 43

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements. What is the MOST cost-effective storage solution for this situation?

- A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
- B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
- C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
- D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

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

- A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
- B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.

- C. Create a new security group that includes the same IP restrictions that exist in the current EC2 securitygroup. Associate this new security group with the CloudFront distribution.
- D. Create a new security group that includes the same IP restrictions that exist in the current EC2 securitygroup. Associate this new security group with the S3 bucket hosting the static content.
- E. Create a new IAM role and associate the role with the distribution. Change the permissions either on theS3 bucket or on the files within the S3 bucket so that only the newly created IAM role has read and download permissions.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

- A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
- B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directorydomain for authentication.

Correct Answer: D

Section: (none)

Explanation

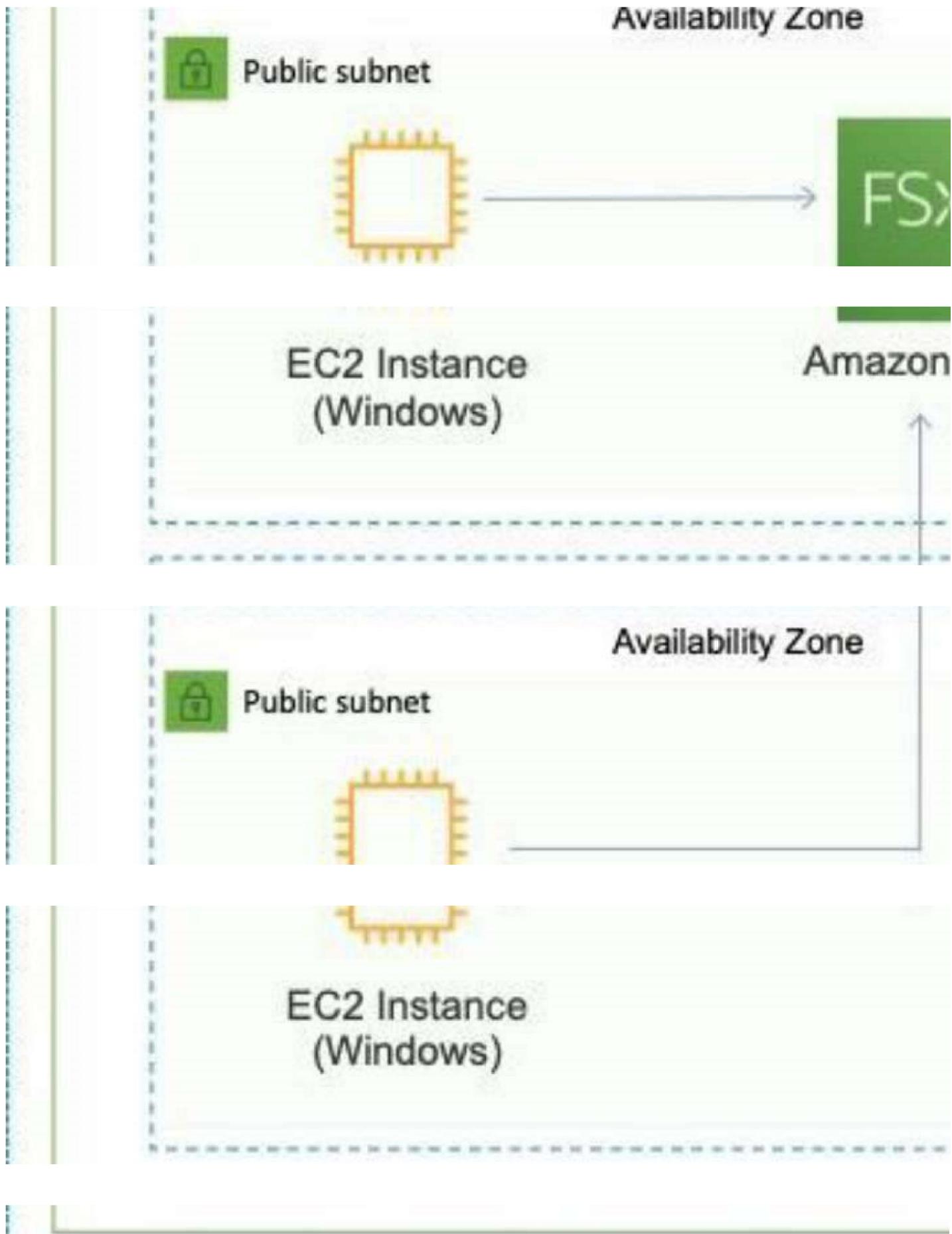
Explanation/Reference:

Explanation



Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi- AZ deployment options, fully managed backups, and encryption of data at rest and in transit. You can optimize cost and performance for your workload needs with SSD and HDD storage options; and you can scale storage and change the throughput performance of your file system at any time. Amazon FSx file storage is accessible from Windows, Linux, and MacOS compute instances and devices running on AWS or on premises.

Works with Microsoft Active Directory (AD) to easily integrate file systems with Windows environments.



CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems. **INCORRECT:** "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.

INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company needs to replace the file server farm and Amazon FSx is the best choice for this job.

References: <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html>

QUESTION 47

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3. How can a solutions architect ensure that the application has permission to access Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
- B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the taskdefinition.
- C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launchconfiguration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

A solutions architect has configured the following IAM policy.

{

"Statement": "0000_10_17"

"Validation": "0000_10_17"

"Statement": [

{

"Statement": "0000_10_17"

"ELEM": "All"

"Action": [

"Lambda": "

"

],

"Resource": "*"

}

for
{

"Effect": "Dem

"Condition": "P
"Action": "L

"Lambda:Cr

"Lambda:Re

"

}

"Resource": "*

"Condition": "P
"Action": "L

"IpAddress

Which action will be allowed by the policy?

- A. An AWS Lambda function can be deleted from any network.
- B. An AWS Lambda function can be created from any network.
- C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.
- D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have been complaining of timeouts. The architecture uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests. How should a solutions architect redesign the architecture to better respond to changing traffic?

- A. Configure a Network Load Balancer with a slow start configuration.
- B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.
- C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
- D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

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

Which configuration will meet this requirement?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS, and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy

processing times. A solutions architect needs to reduce these processing times. Which action will be MOST effective in accomplishing this?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

A company wants to host a web application on AWS that will communicate to a database within a VPC.

The application should be highly available.

What should a solutions architect recommend?

- A. Create two Amazon EC2 instances to host the web servers behind a load balancer, and then deploy the database on a large instance.
- B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.
- C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.
- D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two webservers, and then deploy a database architecture in multiple Availability Zones.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol. Which AWS managed service meets these requirements?

- A. Amazon EBS
- B. Amazon EC2
- C. Amazon FSx
- D. Amazon S3

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.

Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end user file restore, user quotas, and Access Control Lists (ACLs).

Additionally, Amazon FSX for Windows File Server supports Distributed File System Replication (DFSR) in both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.

CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon Elastic Block Store (EBS)" is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application. INCORRECT: "Amazon EC2" is incorrect as no SMB support. INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.

References: <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html>

QUESTION 57

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache that can reduce Amazon DynamoDB response times from milliseconds to microseconds, even at millions of requests per second.

Amazon ElastiCache is incorrect because although you may use ElastiCache as your database cache, it will not reduce the DynamoDB response time from milliseconds to microseconds as compared with DynamoDB DAX.

AWS Device Farm is incorrect because this 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.

DynamoDB Read Replica is incorrect because this is primarily used to automate capacity management for

Read-Through Cache

your tables and global secondary indexes.

References:

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

<https://aws.amazon.com/device-farm>

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/aws-cheat-sheet-amazon-dynamodb/>

Exam D

QUESTION 1

A company wants to use an AWS Region as a disaster recovery location for its on-premises infrastructure. The company has 10 TB of existing data, and the on-premise data center has a 1 Gbps internet connection. A solutions architect must find a solution so the company can have its existing data on AWS in 72 hours without transmitting it using an unencrypted channel. Which solution should the solutions architect select?

- A. Send the initial 10 TB of data to AWS using FTP.
- B. Send the initial 10 TB of data to AWS using AWS Snowball.
- C. Establish a VPN connection between Amazon VPC and the company's data center.
- D. Establish an AWS Direct Connect connection between Amazon VPC and the company's data center.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Keyword: AWS Region as DR for On-premises DC (Existing Data=10TB) + 1G Internet Connection

Condition: 10TB on AWS in 72 Hours + Without Unencrypted Channel

Without Unencrypted Channel = VPN

FTP = Unencrypted Channel

Options - A - Out of race, since this is unencrypted channel & not matching the condition Options - B - Out of race due to the timebound target & order /delivering AWS Snowball device will take time

Options - C - Win th race, using the existing 1G Internet Link we can transfer this 10TB data within 24Hrs using encrypted Channel

Options - D - Out of race due to the timebound target & order /delivering AWS Direct Connect will take time

References: <https://docs.aws.amazon.com/snowball/latest/ug/mailing-storage.html>

<https://tutorialsdojo.com/aws-directconnect/>

<https://tutorialsdojo.com/amazon-vpc/>

QUESTION 2

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

A company decides to migrate its three-tier web application from on premises to the AWS Cloud. The new database must be capable of dynamically scaling storage capacity and performing table joins. Which AWS service meets these requirements?

- A. Amazon Aurora
- B. Amazon RDS for SqlServer
- C. Amazon DynamoDB Streams
- D. Amazon DynamoDB on-demand

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

A company needs to implement a relational database with a multi-Region disaster recovery Recovery Point Objective (RPO) of 1 second and an Recovery Time Objective (RTO) of 1 minute. Which AWS solution can achieve this?

- A. Amazon Aurora Global Database

- B. Amazon DynamoDB global tables.
- C. Amazon RDS for MySQL with Multi-AZ enabled.
- D. Amazon RDS for MySQL with a cross-Region snapshot copy.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cross-Region Disaster Recovery

If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

QUESTION 6

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. <https://aws.amazon.com/secrets-manager/>

QUESTION 8

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

A company must re-evaluate its need for the Amazon EC2 instances it currently has provisioned in an Auto Scaling group. At present, the Auto Scaling group is configured for a minimum of two instances and a maximum of four instances across two Availability zones. A Solutions architect reviewed Amazon CloudWatch metrics and found that CPU utilization is consistently low for the EC2 instances. What should the solutions architect recommend to maximize utilization while ensuring the application remains fault tolerant?

- A. Remove some EC2 instances to increase the utilization of remaining instances.
- B. Increase the Amazon Elastic Block Store (Amazon EBS) capacity of instances with less CPU utilization.
- C. Modify the Auto Scaling group scaling policy to scale in and out based on a higher CPU utilization metric.
- D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost effective, limit the provisioning of into and provide the fastest possible response time. Which combination should a solutions architect recommend to meet these requirements?

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon Dynamo
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balances

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

A company is developing a real-time multiplier game that uses UDP for communications between client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention. Which solution should a solution architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

A company currently has 250 TB of backup files stored in Amazon S3 in a vendor's proprietary format. Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversation. What should a solution architect do to accomplish this?

- A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.
- B. Install the conversion software onto an on-premises virtual machines. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.
- C. Use AWS Snowball Edge device to export the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball devices.
- D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

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

What should a solution architect do to automate the failover process?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/>

QUESTION 15

A company needs to share an Amazon S3 bucket with an external vendor. The bucket owner must be able to access all objects.

Which action should be taken to share the S3 bucket?

- A. Update the bucket to be a Requester Pays bucket
- B. Update the bucket to enable cross-origin resource sharing (COPRS)
- C. Create a bucket policy to require users to grant bucket-owner-full when uploading objects
- D. Create an IAM policy to require users to grant bucket-owner-full control when uploading objects.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

A company uses Amazon S3 as its object storage solution. The company has thousands of S3 it uses to store data. Some of the S3 bucket have data that is accessed less frequently than others. A solutions

architect found that lifecycle policies are not consistently implemented or are implemented partially. resulting in data being stored in high-cost storage. Which solution will lower costs without compromising the availability of objects?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

A solution architect is performing a security review of a recently migrated workload. The workload is a web application that consists of Amazon EC2 instances in an Auto Scaling group behind an Application Load balancer. The solution architect must improve the security posture and minimize the impact of a DDoS attack on resources.

Which solution is MOST effective?

- A. Configure an AWS WAF ACL with rate-based rules. Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the EAF ACL on the CloudFront distribution
- B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. Use the identified information to modify a network ACL to block access.
- C. Enable VPC Flow Logs and store them in Amazon S3. Create a custom AWS Lambda function that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.
- D. Enable Amazon GuardDuty and, configure findings written to Amazon CloudWatch Events with Cloud Watch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS). Have Amazon SNS invoke a custom AWS Lambda function that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18 A company has a custom application running on an Amazon EC2 instance that:

- Reads a large amount of data from Amazon S3
- Performs a multi stage analysis
- Writes the results to Amazon DynamoDB

The application writes a significant number of large temporary files during the multi stage analysis. The process performance depends on the temporary storage performance. What would be the fastest storage option for holding the temporary files?

- A. Multiple Amazon S3 buckets with Transfer Acceleration for storage
- B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization
- C. Multiple Amazon EFS volumes using the Network File System version 4.1 (NFSv4.1) protocol.
- D. Multiple instance store volumes with software RAID 0.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

A solution architect must migrate a Windows internet information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network- attached storage (NAS). The solution architected has proposed migrating the IIS web servers Which replacement to the onpromises filo share is MOST resilient and durable?

- A. Migrate the file Share to Amazon RDS.
- B. Migrate the tile Share to AWS Storage Gateway
- C. Migrate the file Share to Amazon FSx dor Windows File Server.
- D. Migrate the tile share to Amazon Elastic File System (Amazon EFS)

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://aws.amazon.com/fsx/windows/>

QUESTION 20

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The traffic remains in the private IP space. All inter-region traffic is encrypted with no single point of failure, or bandwidth bottleneck.

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

QUESTION 21

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can only create deny rules with network ACLs, it is not possible with security groups. Network ACLs process rules in order from the lowest numbered rules to the highest until they reach and allow or deny. The following table describes some of the differences between security groups and network ACLs:

Security Group

— — — — —

Operates at the instance

Operates at the instance

(interface) level

(interface) level

Therefore, the solutions architect should add a deny rule in the inbound table of the network ACL with a

Supports allow rules only

lower rule number than other rules.

CORRECT: "Add a deny rule in the inbound table of the network ACL with a lower rule number than other

Stateful

rules" is the correct answer.

INCORRECT: "Add a deny rule in the outbound table of the network ACL with a lower rule number than

Evaluates all rules

other rules" is incorrect as this will only block outbound traffic. INCORRECT: "Add a rule in the inbound

Evaluates all rules

table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a

deny rule with a security group. INCORRECT: "Add a rule in the outbound table of the security group to

Applies to an instance only if

deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.

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

associated with a group

acls.html

QUESTION 2

A company is using a VPC peering strategy to connect its VPCs in a single Region to allow for crosscommunication. A recent increase in account creations and VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs. There are also new

requests to create site-to-site VPNs with some of the VPCs. A solutions architect has been tasked with creating a centrally networking setup for multiple accounts, VPNS, and VPNs. Which networking solution meets these requirements?

- A. Configure shared VPCs and VPNs and share to each other
- B. Configure a hub-and-spoke and route all traffic through VPC peering.
- C. Configure an AWS Direct Connect between all VPCs and VPNs.
- D. Configure a transit gateway with AWS Transit Gateway and connected all VPCs and VPNs.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations, it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails. What would allow for automatic recovery of the EC2 instance as quickly as possible?

- A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.
- B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.
- C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, triggered instance recovery.
- D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html>

QUESTION 24

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

A company has multiple AWS accounts, for various departments. One of the departments wants to share an Amazon S3 bucket with all other department. Which solution will require the LEAST amount of effort?

- A. Enable cross-account S3 replication for the bucket
- B. Create a pre signed URL for the bucket and share it with other departments
- C. Set the S3 bucket policy to allow cross-account access to other departments
- D. Create IAM users for each of the departments and configure a read-only IAM policy

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

A company collects temperature, humidity, and atmospheric pressure data in cities across multiple continents. The average volume of data collected per site each day is 500 GB. Each site has a high-speed internet connection. The company's weather forecasting applications are based in a single Region and analyze the data daily.

What is the FASTEST way to aggregate data for all of these global sites?

- A. Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.
- B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- C. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- D. Upload the data to an Amazon EC2 instance in the closest Region. Store the data in an Amazon EBS volume. Once a day take an EBS snapshot and copy it to the centralized Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

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

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDelete",  
            "Effect": "Allow",  
            "Action": [  
                "dynamodb: PutItem",  
                "dynamodb: UpdateItem",  
                "dynamodb: DeleteItem"  
            ],  
            "Resource": "arn:aws:  
        }  
    ]  
}  
  
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "List",  
            "Effect": "Allow",  
            "Action": "dynamodb: ListTables",  
            "Resource": "*"  
        }  
    ]  
}
```

B.

```
    "Sid": "DynamoDBPutItemPolicy",
    "Effect": "Allow",
    "Action": [
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem"
    ],
    "Resource": "arn:aws:dynamodb:  
}
```

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDelete",  
            "Effect": "Allow",  
            "Action": "dynamodb:PutItem",  
            "Resource": "arn:aws:  
        }  
    ]  
},  
  
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDelete",  
            "Effect": "Allow",  
            "Action": "dynamodb:PutItem",  
            "Resource": "arn:aws:  
        }  
    ]  
},
```

Correct Answer: A
Section: (none)
Explanation

"Action": "dynamodb:

Explanation/Reference:

"Resource": "arn:aws:

QUESTION 28

},
,

Application developers have noticed that a production application is very slow when business reporting

"Sid": "PutUpdateDelete",

users run large production reports against the Amazon RDS instance backing the application. the CPU and

"Effect": "Deny",

memory utilization metrics for the RDS instance-d not exceed 60% while the reporting queries are running.

"Action": "dynamodb:

The business reporting users must be able to generate reports without affecting the applications

"Resource": "arn:aws:

performance.

]

Which action will accomplish this?

I

- A. Increase the size of the RDS instance
- B. Create a read replica and connect the application to it.
- C. Enable multiple Availability Zones on the RDS instance
- D. Create a read replication and connect the business reports to it.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

A company's packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution, but wants to future reduce data

transfer costs. The company modify the application's source code. What should a solution architect do to reduce costs?

- A. Use Lambda@Edge to compress the files as they are sent to users.
- B. Enable Amazon S3 Transfer Acceleration to reduce the response times.
- C. Enable caching on the CloudFront distribution to store generated files at the edge.
- D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

B seems more expensive; C does not seem right because they are single use files and will not be needed again from the cache; D multipart mainly for large files and will not reduce data and cost; A seems the best: change the application code to compress the files and reduce the amount of data transferred to save costs.

QUESTION 30

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

What should a solutions architect recommend to the application team? (Select TWO.)

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

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

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

- A. Configure a volume using Amazon EFS Mount the EPS volume to each Windows Instance
- B. Configure AWS Storage Gateway in Volume Gateway mode Mount the volume to each Windows instance
- C. Configure Amazon FSx for Windows File Server Mount the Amazon FSx volume to each WindowsInstance
- D. Configure an Amazon EBS volume with the required size Attach each EC2 instance to the volume Mount the file system within the volume to each Windows instance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deploying on Amazon EC2 instances behind an Application Load balancer in an Auto Scaling group. The company needs the ability shift traffic from resources in one region to another.

What should a solutions architect recommend?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Keyword: Users in those Geographic Locations

Condition: Ability Shift traffic from resources in One Region to Another Region

The following table highlights the key function of each type of routing policy:

Geo-location:

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



Policy	What it Does
Simple	Simple DNS response providing the IP address associated with a name
Failover	If primary is down (based on health checks), routes to secondary destination
Geolocation	Uses geographic location you're in (e.g. Europe) to route you to the closest region
Geoproximity	Routes you to the closest region within a geographic area

Latency	Directs you based on the lowest latency route to resources
Multivalue answer	Returns several IP addresses and functions as a basic load balancer
Weighted Can also protect distribution rights.	Uses the relative weights assigned to resources to determine which to route to.

WEIGHTED

USES THE RELATIVE WEIGHTS ASSIGNED TO RESOURCES TO DETERMINE WHICH TO ROUTE TO.

- Can be used for spreading load evenly between regions.

- If you have multiple records for overlapping regions, Route 53 will route to the smallest

- geographic region.

- You can create a default record for IP addresses that do not map to a geographic location.

The following diagram depicts an Amazon Route 53 Geolocation routing policy configuration:

Name	Type	Value	Health	Geolocation
geolocation.dctlabs.com	A	1.1.1.1	ID	Singapore

geolocation.dctlabs.com	A	2.2.2.2	ID	Default

geolocation.dctlabs.com	A	<i>alb-id</i>	ID	Oceania

Singapore



DNS query

Mexico



Reference:

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

route53/?nc2=h_ql_prod_nt_r53

QUESTION 33

A company has several business systems that require access to data stored in a file share. The business

systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company's legacy on-premises environment and with AWS. Which services meet the business requirements? (Select TWO.)

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon FSx for Windows
- D. Amazon S3
- E. AWS Storage Gateway file gateway

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Keyword: SMB + On-premises

Condition: File accessible from both on-premises and AWS

Amazon FSx for Windows File Server

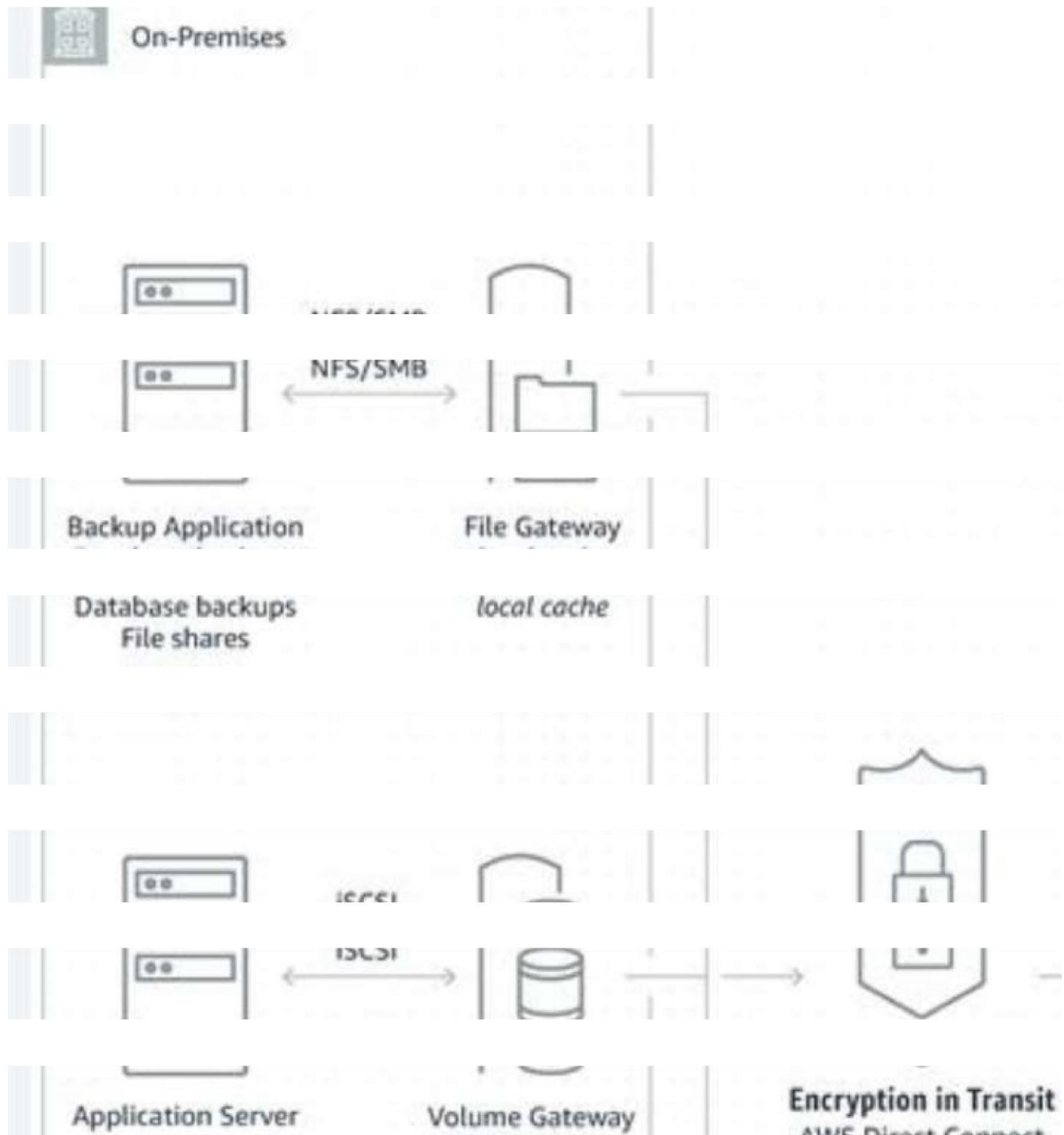
Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit. You can optimize cost and performance for your workload needs with SSD and HDD storage options; and you can scale storage and change the throughput performance of your file system at any time. Amazon FSx file storage is accessible from Windows, Linux, and MacOS compute instances and devices running on AWS or on-premises.

How FSx for Windows File Server works



To support these use cases, Storage Gateway offers three different types of gateways File Gateway, Tape Gateway, and Volume Gateway that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access. Your applications connect to the service through a virtual machine or gateway hardware appliance using standard storage protocols, such as NFS, SMB, and iSCSI. The gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS, and AWS Backup, providing storage for files, volumes, snapshots, and virtual tapes in AWS. The service includes a highly-optimized and efficient data transfer mechanism, with bandwidth management and automated network resilience.

How Storage Gateway works



The table below shows the different gateways available and the interfaces and use cases:

local cache	AWS Direct Connect or Internet
-------------	--------------------------------

CORRECT: "Amazon FSx for Windows" is the correct answer. CORRECT: "Amazon Storage File



Gateway" is the correct answer.



INCORRECT: "Amazon EBS" is incorrect as unsupported NFS/SMB. INCORRECT: "Amazon EFS" is

incorrect as unsupported NFS/SMB. INCORRECT: "Amazon S3" is incorrect as unsupported NFS/SMB.

Backup Application	Tape Gateway local cache
--------------------	-----------------------------

References:

<https://aws.amazon.com/fsx/windows/>

Gateway deployment options:
VMware, Hyper-V, KVM,
or hardware appliance
[https://aws.amazon.com/storagegateway/?whats-new-cards.sort-](https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc)

by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc <https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/> <https://d0.awsstatic.com/whitepapers/aws-storage-gateway/>

New Name	Old Name	Interface	Use Case
File Gateway	None	NFS, SMB	Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount point
Volume Gateway Stored Mode	Gateway-Stored Volumes	iSCSI	Asynchronous replication of on-prem data to S3
Volume Gateway Cached Mode	Gateway-Cached Volumes	iSCSI	Primary data stored in S3 with frequently accessed data cached locally on-prem

QUESTION 34

Tape Gateway	Gateway-Virtual Tape Library	iSCSI	Virtual media changer and tape library for use with existing backup software
--------------	------------------------------	-------	--

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

A company wants to deploy a shared file system for its .NET application servers and Microsoft SQL Server database running on Amazon EC2 instance with Windows Server 2016. The solution must be able to be integrated in to the corporate Active Directory domain, be highly durable, be managed by AWS, and provided levels of throughput and IOPS. Which solution meets these requirements?

- A. Use Amazon FSx for Windows File Server
- B. Use Amazon Elastic File System (Amazon EFS)
- C. Use AWS Storage Gateway in file gateway mode.
- D. Deploy a Windows file server on two On Demand instances across two Availability Zones.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://aws.amazon.com/fsx/windows/>

QUESTION 36

A company is designing a new service that will run on Amazon EC2 instance behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.

What should a solution architect recommend to meet the clients' needs? What should a solution architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an a associated Elastic IP address
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Route 53 routes end users to Internet applications so the correct answer is C. Map one of the whitelisted IP addresses using an A record to the Elastic IP address.

QUESTION 37

A company is designing a new service that will run on Amazon EC2 instance behind an Elastic Load Balancer.

However, many of the web service clients can only reach IP addresses whitelisted on their firewalls. What should a solution architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an associated Elastic IP address
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: https://acloud.guru/forums/aws-csysops-2019/discussion/-LzN1_Aw0dL3Z98CkBs1/Using%20EIP%20for%20ALB

<https://www.bluematador.com/blog/static-ips-for-aws-application-load-balancer>

QUESTION 38

A company is investigating potential solutions that would collect, process, and store users' service usage data.

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

A company runs a web service on Amazon CC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across two Availability zones. The company needs a minimum of four instances at all times to meet the required service level agreement (SLA) while keeping costs low.

If an Availability Zone fails, how can the company remain compliant with the SLA?

- A. Add a target tracking scaling policy with a short cooldown period

- B. Change the Auto Scaling group launch configuration to use a larger instance type
- C. Change the Auto Scaling group to use six servers across three Availability Zones
- D. Change the Auto Scaling group to use eight servers across two Availability Zones

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attribute to an increase in the number of read-only SQL queries triggered by business analysts.

A solution architect needs to solve the problem with minimal changes to the existing web application. What should the solution architect recommend?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

A company is building applications in containers.

The company wants to migrate its on-premises development and operations services from its on-premises data center to AWS.

Management states that production system must be cloud agnostic and use the same configuration and administrator tools across production systems. A solutions architect needs to design a managed solution that will align open-source software.

Which solution meets these requirements?

- A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.
- B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS workers nodes.
- C. Launch the containers on Amazon Elastic Containers service (Amazon ECS) with AWS Fargate instances.
- D. Launch the containers on Amazon Elastic Container Service (Amazon EC) with Amazon EC2 instance worker nodes.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When talking about containerized applications, the leading technologies which will always come up during the conversation are Kubernetes and Amazon ECS (Elastic Container Service). While Kubernetes is an open-sourced container orchestration platform that was originally service.

QUESTION 42

A company is running a two-tier ecommerce website using services. The current architect uses a publish-facing Elastic Load Balancer that sends traffic to Amazon EC2 instances in a private subnet. The

static content is hosted on EC2 instances, and the dynamic content is retrieved from a MYSQL database.

The application is running in the United States. The company recently started selling to users in Europe and Australia.

A solution architect needs to design solution so their international users have an improved browsing experience.

Which solution is MOST cost-effective?

- A. Host the entire website on Amazon S3.
- B. Use Amazon CloudFront and Amazon S3 to host static images.
- C. Increase the number of public load balancers and EC2 instances
- D. Deploy the two-tier website in AWS Regions in Europe and Australia.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

A database is on an Amazon RDS MYSQL 5.6 Multi-AZ DB instance that experience highly dynamic reads. Application developers notice a significant slowdown when testing read performance from a secondary AWS Region.

The developers want a solution that provides less than 1 second of read replication latency.

What should the solutions architect recommend?

- A. Install MySQL on Amazon EC2 in the secondary Region.
- B. Migrate the database to Amazon Aurora with cross-Region replicas.
- C. Create another RDS for MySQL read replica in the secondary.
- D. Implement Amazon ElastiCache to improve database query performance.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

An operations team has a standard that states IAM policies should not be applied directly to users. Some new members have not been following this standard. The operation manager needs a way to easily identify the users with attached policies. What should a solutions architect do to accomplish this?

- A. Monitor using AWS CloudTrail
- B. Create an AWS Config rule to run daily
- C. Publish IAM user changes to Amazon SNS
- D. Run AWS Lambda when a user is modified

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A new AWS Config rule is deployed in the account after you enable AWS Security Hub. The AWS Config rule reacts to resource configuration and compliance changes and send these change items to AWS CloudWatch. When AWS CloudWatch receives the compliance change, a CloudWatch event rule triggers the AWS Lambda function.

QUESTION 45

A company has established a new AWS account.

The account is newly provisioned and no changes have been made to the default settings. The company is concerned about the security of the AWS account root user. What should be done to secure the root user?

- A. Create IAM users for daily administrative tasks. Disable the root user.
- B. Create IAM users for daily administrative tasks.
 - Enable multi-factor authentication on the root user.
- C. Generate an access key for the root user.
 - Use the access key for daily administration tasks instead of the AWS Management Console.
- D. Provide the root user credentials to the most senior solution architect.
 - Have the solution architect use the root user for daily administration tasks.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

A healthcare company stores highly sensitive patient records. Compliance requires that multiple copies be stored in different locations. Each record must be stored for 7 years.

The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter. What should a solutions architect recommend?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

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

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

Correct Answer: D

Section: (none)**Explanation****Explanation/Reference:****QUESTION 48**

A solution architect is designing a hybrid application using the AWS cloud. The network between the on-premises data center and AWS will use an AWS Direct Connect (DX) connection.

The application connectivity between AWS and the on-premises data center must be highly resilient. Which DX configuration should be implemented to meet these requirements?

- A. Configure a DX connection with a VPN on top of it.
- B. Configure DX connections at multiple DX locations.
- C. Configure a DX connection using the most reliable DX partner.
- D. Configure multiple virtual interfaces on top of a DX connection.

Correct Answer: B**Section: (none)****Explanation****Explanation/Reference:****QUESTION 49**

A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandates encryption of data before sending it to Amazon S3.

What should a solution architect recommend to satisfy these requirements?

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

Correct Answer: D**Section: (none)****Explanation****Explanation/Reference:****Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

QUESTION 50

A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day.

A solutions architect has been tasked with designing the MOST cost-effective solution.

Which solution will accomplish this?

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

Correct Answer: C**Section: (none)****Explanation****Explanation/Reference:**

QUESTION 51

A company mandates that an Amazon S3 gateway endpoint must allow traffic to trusted buckets only. Which method should a solutions architect implement to meet this requirement?

- A. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's trusted VPCs
- B. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's S3 gateway endpoint IDs
- C. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that blocks access from any VPC other than the company's trusted VPCs
- D. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

A company is designing a web application using AWS that processes insurance quotes. Users will request quotes from the application.

Quotes must be separated by quote type and must be responded to within 24 hours, and must not be lost. The solution should be simple to set up and maintain. Which solution meets these requirements?

- A. Create multiple Amazon Kinesis data streams based on the quote type.
Configure the web application to send messages to the proper data stream.
Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL)
- B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type.
Configure the web application to publish messages to the SNS topic queue.
Configure each backend application server to work its own SQS queue
- C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic.
Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type.
Configure each backend application server to work its own SQS queue.
- D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver datastreams to an Amazon Elasticsearch Service (Amazon ES) cluster.
Configure the web application to send messages to the proper delivery stream.
Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: <https://docs.aws.amazon.com/sns/latest/dg/sns-message-filtering.html> It all depends on where you want to do the quote type classification i.e. in the app and send to a different/multiple SNS topics (B) or use SNS filtering to do the type classification (C). The question doesn't really give you enough info to make a clear choice but configuring SNS filtering is probably less work and easier to maintain than maintaining app code.

QUESTION 53

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group.

The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds

How can this issue be addressed?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

A company recently released a new type of internet-connected sensor. The company is expecting to sell thousands of sensors, which are designed to stream high volumes of data each second to a central location.

A solutions architect must design a solution that ingests and stores data so that engineering teams can analyze it in near-real time with millisecond responsiveness. Which solution should the solutions architect recommend?

- A. Use an Amazon SQS queue to ingest the data.
Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- B. Use an Amazon SOS queue to ingest the data.
Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.
- C. Use Amazon Kinesis Data Streams to ingest the data.
Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- D. Use Amazon Kinesis Data Streams to ingest the data.
Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://aws.amazon.com/blogs/big-data/analyze-data-in-amazon-dynamodb-using-amazon-sagemaker-for-real-time-prediction/>

QUESTION 56

A company is migrating a NoSQL database cluster to Amazon EC2. The database automatically replicates data to maintain at least three copies of the data. I/O throughput of the servers is the highest priority. Which instance type should a solutions architect recommend for the migration?

- A. Storage optimized instances with instance store
- B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume
- C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled
- D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

A company operates a website on Amazon EC2 Linux instances. Some of the instances are failing. Troubleshooting points to insufficient swap space on the failed instances.

The operations team lead needs a solution to monitor this.

What should a solutions architect recommend?

- A. Configure an Amazon CloudWatch SwapUsage metric dimension.
Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
- B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics.
Monitor SwapUsage metrics in CloudWatch.
- C. Install an Amazon CloudWatch agent on the instances.
Run an appropriate script on a set schedule.
Monitor SwapUtilization metrics in CloudWatch.
- D. Enable detailed monitoring in the EC2 console.
Create an Amazon CloudWatch SwapUtilization custom metric.
Monitor SwapUtilization metrics in CloudWatch.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Exam E

QUESTION 1

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

- A. Configure two AWS Lambda functions to run the applications.
Create an Amazon EC2 instance with an instance store volume to store the data.

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

A company requires a durable backup storage solution for its on-premises database servers while ensuring on-premises applications maintain access to these backups for quick recovery. The company will use AWS storage services as the destination for these backups. A solutions architect is designing a solution with minimal operational overhead. Which solution should the solutions architect implement?

- A. Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket
- B. Back up the databases to an AWS Storage Gateway volume gateway and access it using the Amazon S3 API.
- C. Transfer the database backup files to an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance.
- D. Back up the database directly to an AWS Snowball device and use lifecycle rules to move the data to Amazon S3 Glacier Deep Archive.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address.

The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port 443. Which combination of steps will accomplish this task? (Select TWO.)

- A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
- B. Create a security group with a rule to allow TCP port 443 to destination 0 0 0 0/0.
- C. Update the network ACL to allow TCP port 443 from source 0.0 0 0/0.
- D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
- E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0 0/0 and outbound TCP port 32768-65535 to destination 0 0 0.0/0

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling.

Management is concerned that the company is over-provisioning its infrastructure, especially at the front end of the three-tier application.

A solutions architect needs to ensure costs are optimized without impacting performance. What should the solutions architect do to accomplish this?

- A. Use Auto Scaling with Reserved Instances.
- B. Use Auto Scaling with a scheduled scaling policy.
- C. Use Auto Scaling with the suspend-resume feature
- D. Use Auto Scaling with a target tracking scaling policy.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 6

A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application.

A solutions architect wants to implement a solution that is highly available fault tolerant, and automatically scalable.

What should the solutions architect recommend?

- A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
- B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
- C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.

- D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a NetworkLoad Balancer.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

A solutions architect is working on optimizing a legacy document management application running on Microsoft Windows Server in an on-premises data center. The application stores a large number of files on a network file share. The chief information officer wants to reduce the on-premises data center footprint and minimize storage costs by moving on-premises storage to AWS.

What should the solutions architect do to meet these requirements?

- A. Set up an AWS Storage Gateway file gateway.
- B. Set up Amazon Elastic File System (Amazon EFS)
- C. Set up AWS Storage Gateway as a volume gateway
- D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

A company is processing data on a daily basis.

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

- A. Configure a lifecycle policy to delete the objects after 30 days
- B. Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.
- C. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3Standard-IA) after 30 days
- D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 OneZone-IA) after 30 days.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
- B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Tape Gateway

- Some companies have backup applications that can only work with physical tape drives.
- With Tape Gateway, companies can still use their backup applications while using virtual tape drives.
- Virtual tape Library (VTL)
- Back up data with existing applications.

• Back up data using existing

QUESTION 10

• Works with leading backup

A company wants to replicate its data to AWS to recover in the event of a disaster. Today, a system

• Works with leading backup

administrator has scripts that copy data to a NFS share Individual backup files need to be accessed

with low latency by application administrators to deal with errors in processing. What should a solutions

architect recommend to meet these requirements?

A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share

B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share

C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of

the on-premises NFS share.

D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead

of the on-premises NFS share.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings.

All application components will be deployed on the AWS infrastructure. The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

CloudFront for caching and S3 as the origin. Glacier is used for archiving which is not the case for this scenario.

QUESTION 12

A company that develops web applications has launched hundreds of Application Load Balancers (ALBs) in multiple Regions.

The company wants to create an allow list (or the IPs of all the load balancers on its firewall device. A solutions architect is looking for a one-time, highly available solution to address this request, which will also help reduce the number of IPs that need to be allowed by the firewall. What should the solutions architect recommend to meet these requirements?

- A. Create a AWS Lambda function to keep track of the IPs for all the ALBs in different Regions
Keeprefreshing this list.
- B. Set up a Network Load Balancer (NLB) with Elastic IPs.
Register the private IPs of all the ALBs as targets to this NLB.
- C. Launch AWS Global Accelerator and create endpoints for all the Regions.Register all the ALBs in different Regions to the corresponding endpoints
- D. Set up an Amazon EC2 instance, assign an Elastic IP to this EC2 instance, and configure the instanceas a proxy to forward traffic to all the ALBs.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3.

The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services. Which solution should a solutions architect recommend to keep the data private?

- A. Deploy an AWS DataSync agent for the on-premises environment.
Configure a sync job to replicate the data and connect it with an AWS service endpoint.
- B. Deploy an AWS DataSync agent for the on-premises environment.Schedule a batch job to replicate point-In-time snapshots to AWS.

- C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment.
Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.
- D. Deploy an AWS Storage Gateway file gateway for the on-premises environment.
Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can use AWS DataSync with your Direct Connect link to access public service endpoints or private VPC endpoints. When using VPC endpoints, data transferred between the DataSync agent and AWS services does not traverse the public internet or need public IP addresses, increasing the security of data as it is copied over the network.

QUESTION 14

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs.

The solution must allow for immediate retrieval of data at no additional cost.

How can these requirements be met?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access.

In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

QUESTION 15

A company is reviewing its AWS Cloud deployment to ensure its data is not accessed by anyone without appropriate authorization.

A solutions architect is tasked with identifying all open Amazon S3 buckets and recording any S3 bucket configuration changes.

What should the solutions architect do to accomplish this?

- A. Enable AWS Config service with the appropriate rules.
- B. Enable AWS Trusted Advisor with the appropriate checks.
- C. Write a script using an AWS SDK to generate a bucket report

D. Enable Amazon S3 server access logging and configure Amazon CloudWatch Events.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon CloudWatch Config

- Helps with auditing and recording configuration changes
- Helps record configuration changes
 - Helps record configuration changes
- Possibility of storing the configuration changes in S3

QUESTION 16

• Questions that can be solved

A company built an application that lets users check in to places they visit, rank the places, and add reviews about their experiences.

- Is there unrestricted SSH access to the database?
- Do my buckets have any duplicate data?

The application is successful with a rapid increase in the number of users every month. The chief

technology officer fears the database supporting the current Infrastructure may not handle the new load the

following month because the single Amazon RDS for MySQL instance has triggered alarms related to

• You can receive alerts (SN

resource exhaustion due to read requests. What can a solutions architect recommend to prevent service

• AWS Config is a per-region

Interruptions at the database layer with minimal changes to code?

• AWS Config is a per-region

A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints. Enable a

• Can be aggregated across regions

Multi-AZ deployment.

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

A company runs an application on Amazon EC2 Instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that is highly available across the Region. Which solution should be implemented to ensure that there are no disruptions to Internet connectivity?

- A. Deploy a NAT Instance In a private subnet of each Availability Zone.
- B. Deploy a NAT gateway in a public subnet of each Availability Zone.
- C. Deploy a transit gateway in a private subnet of each Availability Zone.
- D. Deploy an internet gateway in a public subnet of each Availability Zone.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

A company has migrated an on-premises Oracle database to an Amazon RDS (or Oracle Multi- AZ DB instance) In the us-east-1 Region.

A solutions architect is designing a disaster recovery strategy to have the database provisioned In the uswest-2 Region In case the database becomes unavailable in the us-east-1 Region. The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.

How can these requirements be met?

- A. Edit the DB instance and create a read replica in us-west-2.
Promote the read replica to master In us-west-2 in case the disaster recovery environment needs to be activated.
- B. Select the multi-Region option to provision a standby instance in us-west-2.
The standby Instance will be automatically promoted to master In us-west-2 in case the disaster recovery environment needs to be created.
- C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours. Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.
- D. Create a multimaster read/write instances across multiple AWS Regions Select VPCs in us-east-1 andus-west-2 to make that deployment.
Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

A company has an application with a REST-based Interface that allows data to be received in near-real time from a third-party vendor.

Once received, the application processes and stores the data for further analysis.
The application is running on Amazon EC2 instances.
The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application.
When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.
Which design should a solutions architect recommend to provide a more scalable solution?

- A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
- B. Use Amazon API Gateway on top of the existing application.
 - Create a usage plan with a quota limit for the third-party vendor.
- C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data.
 - Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.
- D. Repackage the application as a container.
 - Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

A company recently deployed a two-tier application in two Availability Zones in the us-east-1 Region. The databases are deployed in a private subnet while the web servers are deployed in a public subnet. An internet gateway is attached to the VPC. The application and database run on Amazon EC2 instances. The database servers are unable to access patches on the internet. A solutions architect needs to design a solution that maintains database security with the least operational overhead. Which solution meets these requirements?

- A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with anElastic IP address.
 - Update the routing table of the private subnet to use it as the default route.
- B. Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with anElastic IP address.
 - Update the routing table of the private subnet to use it as the default route.
- C. Deploy two NAT instances inside the public subnet for each Availability Zone and associate them withElastic IP addresses.
 - Update the routing table of the private subnet to use it as the default route.

- D. Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses.
Update the routing table of the private subnet to use it as the default route.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

NAT Gateway

- AWS managed NAT higher performance
- Pay by the hour for usage
- NAT is created in a specific VPC

QUESTION 22

A solutions architect must design a solution for a persistent database that is being migrated from

- Cannot be used by an instance on-premises to AWS.

The database requires 64,000 IOPS according to the database administrator. If possible, the database

- Requires an IGW (Private)

administrator wants to use a single Amazon Elastic Block Store (Amazon EBS) volume to host the

- 5 Gbps of bandwidth with database instance.

- 5 Gbps of bandwidth with

Which solution effectively meets the database administrator's criteria?

- No security group to map

A. Use an instance from the 13 I/O optimized family and leverage local ephemeral storage to achieve

- No security group to map

the IOPS requirement.

B. Create an Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1)

volume attached. Configure the volume to have 64,000 IOPS.

C. Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.

D. Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

EBS – Volume Type

- **gp2: General Purpose Volume**

- 3 IOPS / GiB, minimum 1GiB
- 3000 IOPS / GiB, minimum 10GiB
- 1 GiB = 1TB, 1TB = 1000 GiB
- 1 GiB = 16 TiB, 1TiB = 1000 GiB

- **io1: Provisioned IOPS (expensive)**

- 100 IOPS Minimum
- 100 IOPS Maximum

QUESTION 23

- Min 100 IOPS, Max 64000

A company recently launched its website to serve content to its global user base. The company wants to

- 4 GiB - 16 TiB. Size of vo

store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an

- SSI: Throughput Optimized

Amazon EC2 instance attached as its origin. How should a solutions architect optimize high availability for

- SSI: Throughput Optimized

the application?

- 500 GiB - 16 TiB , 500 Mi

A. Use Lambda@Edge for CloudFront.

- SSI: Cold HDD, Infrequent

B. Use Amazon S3 Transfer Acceleration for CloudFront.

- SSI: Cold HDD, Infrequent

C. Configure another EC2 instance in a different Availability Zone as part of the origin group.

- 500 GiB - 16 TiB , 250 Mi

D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

A company is planning to build a new web application on AWS. The company expects predictable traffic most of the year and very high traffic on occasion. The web application needs to be highly available and fault tolerant with minimal latency. What should a solutions architect recommend to meet these requirements?

- A. Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions, each with oneAmazon EC2 instance.
- B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multipleAvailability Zones.

- C. Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones.
- D. Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

A company wants to migrate a workload to AWS.

The chief information security officer requires that all data be encrypted at rest when stored in the cloud.

The company wants complete control of encryption key lifecycle management. The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail.

The chosen services should integrate with other storage services that will be used on AWS. Which services satisfies these security requirements?

- A. AWS CloudHSM with the CloudHSM client
- B. AWS Key Management Service (AWS KMS) with AWS CloudHSM
- C. AWS Key Management Service (AWS KMS) with an external key material origin
- D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Took a bit of reading. Key points in question:

"The company must be able to immediately remove the key material and audit key usage independently"

"The chosen services should integrate with other storage services that will be used on AWS" Point 1: Q:

Can I use CloudHSM to store keys or encrypt data used by other AWS services? Ans: Yes. You can do all encryption in your CloudHSM-integrated application. In this case, AWS services such as Amazon S3 or Amazon Elastic Block Store (EBS) would only see your data encrypted.

Point 2: AWS manages the hardware security module (HSM) appliance, but does not have access to your keys. You control and manage your own keys Ref: <https://aws.amazon.com/cloudhsm/features/> Ref: <https://aws.amazon.com/cloudhsm/faqs/>

QUESTION 26

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts.

The company has created a central AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users.

The solution must be secure and optimized. How should a solutions architect meet these requirements?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

A company has an application that posts messages to Amazon SQS. Another application polls the queue and processes the messages in an I/O-intensive operation. The company has a service level agreement (SLA) that specifies the maximum amount of time that can elapse between receiving the messages and responding to the users. Due to an increase in the number of messages the company has difficulty meeting its SLA consistently.

What should a solutions architect do to help improve the application's processing time and ensure it can handle the load at any level?

- A. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with a larger size.
- B. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with an Amazon EC2 Dedicated Instance
- C. Create an Amazon Machine image (AMI) from the instance used for processing.
Create an Auto Scaling group using this image in its launch configuration.
Configure the group with a target tracking policy to keep us aggregate CPU utilization below 70%.
- D. Create an Amazon Machine Image (AMI) from the instance used for processing.
Create an Auto Scaling group using this image in its launch configuration.
Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

A company is planning to deploy an Amazon RDS DB instance running Amazon Aurora. The company has a backup retention policy requirement of 90 days. Which solution should a solutions architect recommend?

- A. Set the backup retention period to 90 days when creating the RDS DB instance
- B. Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecyclepolicy set to delete after 90 days.
- C. Create an AWS Backup plan to perform a daily snapshot of the RDS database with the retention set to90 days.
Create an AWS Backup job to schedule the execution of the backup plan daily
- D. Use a daily scheduled event with Amazon CloudWatch Events to execute a custom AWS Lambdafunction that makes a copy of the RDS automated snapshot Purge snapshots older than 90 days

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

A company is using a tape backup solution to store its key application data offsite.

The daily data volume is around 50 TB.

The company needs to retain the backups for 7 years for regulatory purposes. The backups are rarely accessed and a week's notice is typically given if a backup needs to be restored.

The company is now considering a cloud-based option to reduce the storage costs and operational burden of managing tapes.

The company also wants to make sure that the transition (rom tape backups to the cloud minimizes disruptions).

Which storage solution is MOST cost-effective'?

- A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive
- B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.
- C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier
- D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move thebackup to Amazon S3 Glacier

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

It requires HA and if one AZ is down then at least 4 instances will be active in another AZ which is key for this question.

QUESTION 33

A company is planning to migrate its virtual server-based workloads to AWS. The company has internet-facing load balancers backed by application servers. The application servers rely on patches from an internet-hosted repository. Which services should a solutions architect recommend be hosted on the public subnet? (Select TWO.)

- A. NAT gateway
- B. Amazon RDS DB instances
- C. Application Load Balancers
- D. Amazon EC2 application servers
- E. Amazon Elastic File System (Amazon EFS) volumes

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

An application is running on Amazon EC2 instances. Sensitive information required for the application is stored in an Amazon S3 bucket.

The bucket needs to be protected from internet access while only allowing services within the VPC access to the bucket.

Which combination of actions should a solutions architect take to accomplish this? (Select TWO.)

- A. Create a VPC endpoint for Amazon S3.

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

ACL is a property at object level not at bucket level .Also by just adding ACL you cant let the services in VPC allow access to the bucket .

QUESTION 35

A solutions architect is designing a multi-Region disaster recovery solution for an application that will provide public API access.

The application will use Amazon EC2 instances with a userdata script to load application code and an Amazon RDS for MySQL database.

The Recovery Time Objective (RTO) is 3 hours and the Recovery Point Objective (RPO) is 24 hours.

Which architecture would meet these requirements at the LOWEST cost?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users.

The volume of requests is highly variable, several hours can pass without receiving a single request. The data processing will take place asynchronously but should be completed within a few seconds after a request is made

Which compute service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?

- A. An AWS Glue job
- B. An AWS Lambda function
- C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)
- D. A containerized service hosted in Amazon ECS with Amazon EC2

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client side JavaScript, and images. Which method is the MOST costeffective for hosting the website?

- A. Containerize the website and host it in AWS Fargate
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express framework

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

A company has media and application files that need to be shared internally. Users currently are authenticated using Active Directory and access files from a Microsoft Windows platform.

The chief executive officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit. What should a solutions architect recommend?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

A company is moving its legacy workload to the AWS Cloud. The workload files will be shared, appended, and frequently accessed through Amazon EC2 instances when they are first created. The files will be accessed occasionally as they age. What should a solutions architect recommend?

- A. Store the data using Amazon EC2 instances with attached Amazon Elastic Block Store (Amazon EBS) data volumes
- B. Store the data using AWS Storage Gateway volume gateway and export rarely accessed data to Amazon S3 storage
- C. Store the data using Amazon Elastic File System (Amazon EFS) with lifecycle management enabled for rarely accessed data
- D. Store the data using Amazon S3 with an S3 lifecycle policy enabled to move data to S3 Standard-Infrequent Access (S3 Standard-IA)

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

A company is deploying a multi-instance application within AWS that requires minimal latency between the instances.

What should a solutions architect recommend?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

A company runs a high performance computing (HPC) workload on AWS. The workload required lowlatency network performance and high network throughput with tightly coupled node-to-node communication.

The Amazon EC2 instances are properly sized for compute and storage capacity, and are launched using default options.

What should a solutions architect propose to improve the performance of the workload?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45 A company's dynamic website is hosted using on-premises servers in the United States.

The company is launching its product in Europe and it wants to optimize site loading times for new European users.

The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed

What should the solutions architect recommend?

- A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it
- B. Move the website to Amazon S3 Use cross-Region replication between Regions.
- C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers
- D. Use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

A company is building a media-sharing application and decides to use Amazon S3 for storage. When a media file is uploaded the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions and extract and store the metadata to an Amazon DynamoDB table.

The metadata is used for searching and navigation. The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses. What should a solutions architect recommend to support this workload?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

A company has recently updated its internal security standards. The company must now ensure all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists.

The company is looking for a native, software-based AWS service to accomplish this goal. What should a solutions architect recommend as a solution?

- A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.
- B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store masterkey material and apply a routine to re-create a new key periodically and replace it in AWS KMS.
- C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the CloudHSM cluster nodes.
- D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) to store masterkey material and apply a routine to re-create a new key periodically and replace it in the Parameter Store.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AWS Secrets Manager provides full lifecycle management for secrets within your environment. In this post, Maitreya and I will show you how to use Secrets Manager to store, deliver, and rotate SSH keypairs used for communication within compute clusters. Rotation of these keypairs is a security best practice, and sometimes a regulatory requirement. Traditionally, these keypairs have been associated with a number of

tough challenges. For example, synchronize key rotation across all compute nodes, enable detailed logging and auditing, and manage access to users in order to modify secrets.

QUESTION 48

A solution architect must design a solution that uses Amazon CloudFront with an Amazon S3 to store a static website.

The company security policy requires that all websites traffic be inspected by AWS WAF. How should the solution architect company with these requirements?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

A company has copied 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region using an AWS Direct Connect link.

The company now wants to copy the data to another S3 bucket in the us-west-2 Region. The colocation facility does not allow the use AWS Snowball. What should a solutions architect recommend to accomplish this?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named Company Confidential.

The cloud engineer must be able to read from and write to an S3 bucket called AdminTools.

Which IAM policy will meet these requirements?

A.

"Resource": "arn:aws:

},
}

"Effect": "Allow",

"Action": ["s3:GetOb

"Resource": "arn:aws:

},
}

"Effect": "Deny",

"Action": "s3:Get",

"Resource": [

"arn:aws:s3:::Com

"arn:aws:s3:::Com

]

B.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3:listBucket",  
            "Resource": [  
                "arn:aws:s3:::AdminTool",  
                "arn:aws:s3:::CompanyC  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject" ],  
            "Resource": "  
        }  
        {"Effect": "Deny",  
}
```


D.

```
        "arn:aws:s3:::Compar
        "arn:aws:s3:::Compar
[{"Effect": "Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::Compar"}, {"Effect": "Allow", "Action": ["s3:GetObject"], "Resource": "arn:aws:s3:::Compar"}]
```

```
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": [
        "arn:aws:s3:::Company",
        "arn:aws:s3:::Company",
        "arn:aws:s3:::AdminTo"
    ]
}
```

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 51

An engineering team is developing and deploying AWS Lambda functions. The team needs to create roles and manage policies in AWS IAM to configure the permissions of the Lambda functions.

How should the permissions for the team be configured so they also adhere to the concept of least privilege?

- A. Create an IAM role with a managed policy attached.
Allow the engineering team and the Lambda functions to assume this role
- B. Create an IAM group for the engineering team with an IAMFullAccess policy attached. Add all the users from the team to this IAM group
- C. Create an execution role for the Lambda functions.
Attach a managed policy that has permission boundaries specific to these Lambda functions
- D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions.
Allow the engineering team to assume this role.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 52

A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly.

What is the MOST cost-effective method to establish this type of connection?

- A. Implement a client VPN
- B. Implement AWS Direct Connect
- C. Implement a bastion host on Amazon EC2 53D.
- D. Implement an AWS Site-to-Site VPN connection.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

A company is building a payment application that must be highly available even during regional service disruptions.

A solutions architect must design a data storage solution that can be easily replicated and used in other AWS Regions.

The application also requires low-latency atomicity, consistency, isolation, and durability (ACID) transactions that need to be immediately available to generate reports.

The development team also needs to use SQL.

Which data storage solution meets these requirements'?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application.

The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

A company uses a legacy on-premises analytics application that operates on gigabytes of csv files and represents months of data.

The legacy application cannot handle the growing size of csv files. New csv files are added daily from various data sources to a central on-premises storage location. The company wants to continue to support the legacy application while users learn AWS analytics services.

To achieve this, a solutions architect wants to maintain two synchronized copies of all the csv files on-premises and in Amazon S3.

Which solution should the solutions architect recommend?

- A. Deploy AWS DataSync on-premises.

Configure DataSync to continuously replicate the csv files between the company's on-premises storage and the company's S3 bucket

- B. Deploy an on-premises file gateway.

Configure data sources to write the csv files to the file gateway.

Point the legacy analytics application to the file gateway.

The file gateway should replicate the csv files to Amazon S3

- C. Deploy an on-premises volume gateway.

Configure data sources to write the csv files to the volume gateway.

Point the legacy analytics application to the volume gateway.

The volume gateway should replicate data to Amazon S3.

- D. Deploy AWS DataSync on-premises.

Configure DataSync to continuously replicate the csv files between on-premises and Amazon Elastic File System (Amazon EFS).

Enable replication from Amazon EFS to the company's S3 bucket.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic.

A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment.

Serve the read requests from the primary Availability Zone.

- B. Change the existing database to a Multi-AZ deployment.

Serve the read requests from the secondary Availability Zone.

- C. Create read replicas for the database.

Configure the read replicas with half of the compute and storage resources as the source database.

- D. Create read replicas for the database.

Configure the read replicas with the same compute and storage resources as the source database.

Correct Answer: D

Section: (none)

Explanation

• Read Replicas

Explanation/Reference:

Explanation:

- You have a production database that is taking on normal load that is causing performance issues.
- You want to run a reporting application to run some analysis.
- You don't want to affect the production database.
- You create a Read Replica to handle the new workload there.
- The production application is unaffected.

QUESTION 57

- Read replicas are used for SE

A company wants to optimize the cost of its data storage for data that is accessed quarterly. The company

requires high throughput, low latency, and rapid access, when needed. Which Amazon S3 storage class

should a solutions architect recommend?

A. Amazon S3 Glacier (S3 Glacier)

B. Amazon S3 Standard (S3 Standard)

C. Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

D. Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Exam F

QUESTION 1

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

S3 – Moving between storage classes

- You can transition objects between storage classes

- For infrequently accessed objects move them to 'STANDARD'
 - For seldom accessed objects you don't need in real time, GLACIER
 - For archive objects you don't need in real-time, GLACIER or DEEP_ARCHIVE
-
- Moving objects can be automated
 - Moving objects can be automated using a lifecycle configuration

S3 Storage Classes

Example us-east-2

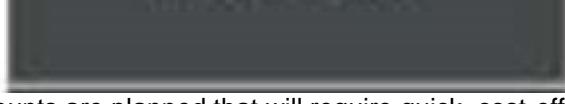
	S3 Standard	S3 Intelligent-Tiering
Storage Cost	\$0.0125 -	
(per GB per month)	\$0.023	\$0.023
Retention		

QUESTION 2**Retrieval Cost**

A company hosts its core network services, including directory services and DNS, in its on-premises data center.

Retrieval Cost (per 1000 requests)**GET****(per 1000 requests)****GET \$0.0004****\$0.0004**

The data center is connected to the AWS Cloud using AWS Direct Connect (DX). Additional AWS



accounts are planned that will require quick, cost-effective, and consistent access to these network



services. What should a solutions architect implement to meet these requirements with the LEAST amount

of operational overhead?



- A. Create a DX connection in each new account.



Route the network traffic to the on-premises servers



- B. Configure VPC endpoints in the DX VPC for all required services.



Route the network traffic to the on-premises servers

- C. Create a VPN connection between each new account and the DX VPC. Route the network traffic to the on-premises servers
- D. Configure AWS Transit Gateway between the accounts.

Assign DX to the transit gateway and route network traffic to the on-premises servers

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Transit Gateway

- For having transitive peering between the on-premises, hub-and-spoke (star) connection
- Regional resource, can work cross-region
- Share cross-account using Resource Access Manager
- You can peer Transit Gateways across regions
- Route Tables: limit which VPC can talk with each other

- Works with Direct Connect Gateway, VPC peering, and AWS Lambda
- Supports IP Multicast (not supported by some services)

QUESTION 3

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon

RDS DB instances and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check. What should a solutions architect do to accomplish this?"

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

Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AWS Config Rule

AVVS Config Rule

- Can use AVVS managed config rules
 - Evaluate if each EBS disk is of type gp2
 - Evaluate if each EC2 instance is running in a VPC
- Rules can be evaluated / triggered
 - For each config change
 - And / or: at regular time intervals
 - Can trigger CloudWatch Events

QUESTION 4

- Rules can have auto remediation.

An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table. Both

the EC2 instance and the DynamoDB table are in the same AWS account. A solutions architect must

configure the necessary permissions. Which solution will allow least privilege access to the DynamoDB

table from the EC2 instance?

- AWS Config Rules does not

A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an

- Pricing: no free tier. \$2 per ad

instance profile to assign this IAM role to the EC2 instance

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

An application uses an Amazon RDS MySQL DB instance.

The RDS database is becoming low on disk space.

A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

- A. Enable storage auto scaling in RDS.
- B. Increase the RDS database instance size
- C. Change the RDS database instance storage type to Provisioned IOPS.

- D. Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Advantage over using DB on EC2

- RDS is a managed service:
 - Automated provisioning, OS patching, monitoring
 - Continuous backups and restores
 - Monitoring dashboards
 - Read replicas for improved read scalability

- Multi AZ setup for DR (Disaster Recovery)
- Maintenance windows for updates
- Scaling capability (vertical and horizontal)
- Storage backed by EBS (gp2)

QUESTION 6

- BUT you can't SSH into your instances

A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only. What should a solutions architect do to protect against data loss? (Choose two.)

- A. Enable versioning on the S3 bucket.
- B. Enable access logging on the S3 bucket.
- C. Enable server-side encryption on the S3 bucket.
- D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.
- E. Use MFA Delete to require multi-factor authentication to delete an object.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

VPC Endpoints

- Endpoints allow you to connect to services inside your VPC instead of the public www network
- They scale horizontally and are highly available
- They remove the need of IGW
- Interface: provisions an ENI (private IP) and attach security group) – most common
- Gateway: provisions a target endpoint (AWS Lambda, DynamoDB)
- In case of issues:

QUESTION 8

- Check DNS Setting Resolution
- Check Route Tables

A company is designing a message-driven order processing application on AWS. The application consists of many services and needs to communicate the results of its processing to multiple consuming services. Each of the consuming services may take up to 5 days to receive the messages.

Which process will meet these requirements?

- A. The application sends the results of its processing to an Amazon Simple Notification Service (AmazonSNS) topic.
Each consuming service subscribes to this SNS topic and consumes the results
- B. The application sends the results of its processing to an Amazon Simple Notification Service (AmazonSNS) topic.
Each consuming service consumes the messages directly from its corresponding SNS topic.
- C. The application sends the results of its processing to an Amazon Simple Queue Service (Amazon SQS) queue.
Each consuming service runs as an AWS Lambda function that consumes this single SQS queue.
- D. The application sends the results of its processing to an Amazon Simple Notification Service (AmazonSNS) topic.
An Amazon Simple Queue Service (Amazon SQS) queue is created for each service and each queue is configured to be a subscriber of the SNS topic.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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

Which solution is MOST cost-effective?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it.

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

EC2 Spot Instances

- Can get a discount of up to 90%
- Instances that you can “lose” at

current spot price

- The **MOST** cost-efficient instance
- The **MOST COST-EFFICIENT INSTANCE** is the current spot price
- Useful for workloads that are **non-critical**
 - Batch jobs
 - Data analysis
 - Image processing
 - ...
- Not great for critical jobs or data
- Great combo: Reserved Instances
- Great combo: Reserved Instances

QUESTION 11

An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service free and paid. Photos submitted by paid users are processed before those submitted by free users.

Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS. Which configuration should a solutions architect recommend?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions.

To communicate with each other, the instances use the internet for connectivity. The security team wants to ensure that no communication between the instances happens over the internet. What should a solutions architect do to accomplish this?

- A. Create a NAT gateway and update the route table of the EC2 instances' subnet
- B. Create a VPC endpoint and update the route table of the EC2 instances' subnet
- C. Create a VPN connection and update the route table of the EC2 instances' subnet
- D. Create a VPC peering connection and update the route table of the EC2 instances' subnet

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel.

The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime. Which solution meets these requirements MOST cost-effectively?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

EC2 Spot Instances

- Can get a discount of up to 90%
- Instances that you can “lose” at current spot price
- The MOST cost-efficient instances
- Useful for workloads that are re

- Batch jobs

QUESTION 14

- Data analysis

A company with facilities in North America, Europe, and Asia is designing new distributed application to

- Image processing

optimize its global supply chain and manufacturing process. The orders booked on one continent should be

visible to all Regions in a second or less. The database should be able to support failover with a short

- Not great for critical jobs or dat

Recovery Time Objective (RTO). The uptime of the application is important to ensure that manufacturing is

not impacted.

- Great combo: Reserved Instances

What should a solutions architect recommend?

- Great combo: Reserved Instances

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cross-Region Disaster Recovery

If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

- **Cross-Region DR and BC**
- **Global Read Scaling - Low Latency**
- **Global Read Scaling - Low Latency**
- ~1s or less replication between regions
- **No impact** on DB performance
- Secondary regions can have different configurations

- .. Can be promoted to R/W

QUESTION 15

- Currently MAX 5 secondary

A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly. Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.

What should a solutions architect do to optimize costs?

- A. Create an additional NAT gateway Update the route table to route to the NAT gateway.Update the network ACL to allow S3 traffic
- B. Create an internet gateway Update the route table to route traffic to the internet gateway.Update the network ACL to allow S3 traffic.
- C. Create a VPC endpoint for Amazon S3 Attach an endpoint policy to the endpoint.Update the route table to direct traffic to the VPC endpoint
- D. Create an AWS Lambda function outside of the VPC to handle S3 requests.
Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video file has become popular and a large number of users across the world are accessing this content. This has resulted in a cost increase.

Which action will DECREASE cost without compromising user accessibility?

- A. Change the EBS volume to Provisioned IOPS (PIOPS).
- B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.
- C. Split the video into multiple, smaller segments so users are routed to the requested video segments only.
- D. Clear an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

A solutions architect is designing the cloud architecture for a new application being deployed to AWS. The application allows users to interactively download and upload files. Files older than 2 years will be accessed less frequently. The solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend? (Choose two.)

- A. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.
- B. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard-Infrequent Access (S3 Standard-IA)
- C. Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).
- D. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.
- E. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.aws.amazon.com/efs/latest/ug/enable-lifecycle-management.html> <https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

QUESTION 19

A company is hosting multiple websites for several lines of business under its registered parent domain. Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on

the subdomain. The websites host static webpages, images, and server-side scripts like PHP and JavaScript.

Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.

Which combination of AWS services or features will meet these requirements? (Choose two.)

- A. AWS Batch
- B. Network Load Balancer
- C. Application Load Balancer
- D. Amazon EC2 Auto Scaling
- E. Amazon S3 website hosting

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

<https://medium.com/awesomedotcloud/aws-difference-between-application-load-balancer-and-network-load-balancer-cb8b6cd296a4>

QUESTION 20

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

What should the solutions architect do to reduce the overall data transfer costs?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

There is no data transfer cost between eC2 & S3 with in same region.

QUESTION 21

A company is hosting an election reporting website on AWS for users around the world. The website uses Amazon EC2 instances for the web and application tiers in an Auto Scaling group with Application Load Balancers. The database tier uses an Amazon RDS for MySQL database. The website is updated with election results once an hour and has historically observed hundreds of users accessing the reports.

The company is expecting a significant increase in demand because of upcoming elections in different countries. A solutions architect must improve the website's ability to handle additional demand while minimizing the need for additional EC2 instances.

Which solution will meet these requirements?

- A. Launch an Amazon ElastiCache cluster to cache common database queries.

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

A company is running a three-tier web application to process credit card payments. The front-end user interface consists of static webpages. The application tier can have long-running processes. The database tier uses MySQL.

The application is currently running on a single, general purpose large Amazon EC2 instance. A solutions architect needs to decouple the services to make the web application highly available.

Which solution would provide the HIGHEST availability?

- A. Move static assets to Amazon CloudFront.
Leave the application in EC2 in an Auto Scaling group.
Move the database to Amazon RDS to deploy Multi-AZ.
- B. Move static assets and the application into a medium EC2 instance.
Leave the database on the large instance.
Place both instances in an Auto Scaling group.
- C. Move static assets to Amazon S3, Move the application to AWS Lambda with the concurrency limit set.
Move the database to Amazon DynamoDB with on-demand enabled.
- D. Move static assets to Amazon S3.
Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled.
Move the database to Amazon RDS to deploy Multi-AZ.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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

What should a solutions architect recommend?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Rate limit

For a rate-based rule, enter the maximum number of requests to allow in any five-minute period from an IP address that matches the rule's conditions. The rate limit must be at least 100.

You can specify a rate limit alone, or a rate limit and conditions. If you specify only a rate limit, AWS WAF places the limit on all IP addresses. If you specify a rate limit and conditions, AWS WAF places the limit on IP addresses that match the conditions.

When an IP address reaches the rate limit threshold, AWS WAF applies the assigned action (block or count) as quickly as possible, usually within 30 seconds. Once the action is in place, if five minutes pass with no requests from the IP address, AWS WAF resets the counter to zero.

QUESTION 24

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

How can this issue be addressed?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 25**

A company is hosting its static website in an Amazon S3 bucket, which is the origin for Amazon CloudFront. The company has users in the United States, Canada, and Europe and wants to reduce.

What should a solutions architect recommend?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 26**

A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video files has become popular and a large number of user across the world are accessing this content. This has resulted in a cost increase.

Which action will DECREASE cost without compromising user accessibility?

- A. Change the EBS volume to provisioned IOPS (PIOPS)
- B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution
- C. Split the video into multiple, smaller segments so users are routed to the requested video segments only
- D. Create an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

A company built a new VPC with the intention of hosting Amazon EC2 based workloads on AWS. A solutions architect specified that an Amazon S3 gateway endpoint be created and attached to this new VPC. Once the first Application server is built, developers report that server times out when accessing data stored in the S3 bucket.

Which scenario could be causing this issue? (Select TWO)

- A. The S3 bucket is in a region other than the VPC
- B. The endpoint has a policy that blocks the CIDR of the VPC
- C. The route to the S3 endpoint is not configured in the route table
- D. The access is routed through an internet gateway rather than the endpoint
- E. The S3 bucket has a bucket policy that does not allow access to the CIDR of the VPC

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

A solution architect is designing a shared storage solution for an Auto Scaling web application. The company anticipates making frequent changes to the content, so the solution must have strong consistency.

Which solution requires the LEAST amount of effort?

- A. Create an Amazon S3 bucket to store the web content and use Amazon Cloudfront to deliver the content
- B. Create an Amazon Elastic File system (Amazon EFS) file system and mount it on the individual Amazon EC2 instance
- C. Create a shared Amazon Elastic Block store (Amazon EBS) volume and mount it on the individual Amazon EC2 instance
- D. Use AWS DataSync to perform continuous synchronization of data between Amazon EC2 hosts in the Auto scaling group.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

A solution architect creating an application that will handle batch processing of large amount of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solution architect do to reduce the overall data transfer costs ?

- A. Place all the EC2 instances in an Auto scaling group.
- B. Place all the EC2 instance in the same AWS Region
- C. Place all the EC2 instance in the same Availability Zone
- D. Place all the EC2 instances in private subnets in multiple Availability zones

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

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

Which solution provides the LOWEST data transfer egress cost for the company?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

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

What should the solutions architect do to accomplish this?

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

Correct Answer: B

Section: (none)**Explanation****Explanation/Reference:****QUESTION 32**

A company uses a legacy on-premises analytics application that operate on gigabytes of .csv and represents months of data. The legacy application cannit handle the growing size of .csv files. New CSV files added daily from various data sources to a central on-premises storage location. The company wants to continuew to support the legacy application while user learn AWS analytics services. To achieve this, a solution architect wants to maintain two synchronizes copies of all the .csv files on-premises and in Amazon S3.

Which solution should the solution architect recommend?

- A. Deploy AWS Datasync on-premises.configure Datasync to continuously replicate the .csv files betweenthe company's S3 bucket.
- B. Deploye an on-premises file gateway, Configur data source to write the .csv files to the file gateway,point the legacy analytics application to the file gatway. The file gaeway should replicate the .csv file to Amazon S3.
- C. Deploy an on-premises volume gateway.configure data source to write the .csv files to the volumegateway.Point the legacy analytics application to the volume gateway. The volume gateway should replicate data to Amazon S3.
- D. Deploy AWS datasync on-premises. Configure datasync to continuously replicate the .csv files betweenon-premises and Amazon Elastic file system (Amazon EFS) enable replication from Amazon EFS to the comapny's S3 Bucket.

Correct Answer: A**Section: (none)****Explanation****Explanation/Reference:****QUESTION 33**

Management has decided to deploy all AWS VPCs with IPv6 enabled. After sometime, a solutions architect tries to launch a new instance and receives an error stating that there is no enough IP address space available in the subnet.

What should the solutions architect do to fix this?

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

Correct Answer: C**Section: (none)****Explanation****Explanation/Reference:****QUESTION 34**

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

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

Which solution meets these requirements?

- A. The requests from the API are sent to an Application Load Balancer (ALB). Models are deployed as AWS Lambda functions invoked by the ALB
- B. The requests from the API are sent to the model's Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as AWS Lambda functions triggered by SQS events. AWS Auto Scaling is enabled on Lambda to increase the number of vCPUs based on the SQS queue size.
- C. The requests from the API are sent to the model's Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue. AWS App Mesh scales the instances of the ECS cluster based on the SQS queue size.
- D. The requests from the API are sent to the model's Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue. AWS Auto Scaling is enabled for both the cluster and copies the service based on the queue size.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity, developer noticed slowdowns related to the game's metadata load times. Performance metrics indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots, replication, and sub-millisecond response times.

What should the solutions architect recommend to solve the issues?

- A. Migrate the database to Amazon Aurora with Aurora Replicas.
- B. Migrate the database to Amazon DynamoDB with global tables.
- C. Add an Amazon ElastiCache for Redis layer in front of the database.
- D. Add an Amazon ElastiCache for Memcached layer in front of the database.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

A company runs an application that uses multiple Amazon EC2 instances to gather data from its users. The data is then processed and transferred to Amazon S3 for long-term storage. A review of the application shows that there were long periods of time when the EC2 instances were not being used. A solution architect needs to design a solution that optimizes utilization and reduces costs.

Which solution meets these requirements?

- A. Use Amazon EC2 in an Auto Scaling group with On-Demand instances.
- B. Build the application to use Amazon Lightsail with On-Demand instances.

- C. Create an Amazon CloudWatch cron job to automatically stop the EC2 instance when there is no activity.
- D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (AmazonSQS) and AWS Lambda.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IP 4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zone (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable Internet access for the private subnets?

- A. Create three NAT gateways, one for each public subnet in each AZ.

Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.

- B. Create three NAT gateways, one for each private subnet in each AZ.

Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.

- C. Create second internet gateway on one of the private subnets.

Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.

- D. Create an egress-only internet gateway on one of the public subnets.

Update the route table for the private subnets that forward non-VPC traffic to the egress-only internet gateway.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

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

Which solution meets these requirements?

- A. Create an Amazon EFS file system.

Configure a mount target in each Availability Zone.

Attach each instance to the appropriate mount target.

- B. Create an additional EC2 instance and configure it as a file server.

Create a security group that allows communication between the instances and apply that to the additional instance.

- C. Create an Amazon S3 bucket with the appropriate permissions.

Create a role in AWS IAM that grants the correct permissions to the S3 bucket.

Attach the role to the EC2 instances that need access to the data.

- D. Create an Amazon EBS volume with the appropriate permissions.

Create a role in AWS IAM that grants the correct permissions to the EBS volume.

Attach the role to the EC2 instances that need access to the data.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solution architect do to ensure the system can automatically scale for the increased traffic? (Select TWO.)

- A. Configure storage auto scaling on the RDS for Oracle instance.
- B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
- C. Configure an alarm on the RDS for Oracle instance for low free storage space.
- D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
- E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

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

Which solution meets these requirements?

- A. Enable Amazon Guard Duty on the account
- B. Enable Amazon Inspector on the EC2 instances
- C. Enable AWS Shield and assign Amazon Route 53 to it.
- D. Enable AWS Shield Advanced and assign the ELB to it.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

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

What should a solutions architect recommend?

- A. Set up a new Direct Connect connection in another AWS Region.

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

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

Which storage solution meets these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

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

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

- A. AWS S3 Glacier
- B. AWS DataSync
- C. AWS Snowball Edge
- D. AWS Storage Gateway

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/CreatingAnSMBFileShare.html>

QUESTION 44

A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data. The application cannot be modified to use any other communication protocols other than NFS for this purpose.

Which storage solution should a solutions architect recommend for use after the migration?

- A. AWS DataSync
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon Elastic File System (Amazon EFS)
- D. Amazon EMR File System (Amazon EMRFS)

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 45

A company has a dynamic web application hostes on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

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

Which action meets these requirements?

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

Correct Answer: C

Section: (none)**Explanation****Explanation/Reference:****QUESTION 47**

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

What should a solution architect recommend to support this workload?

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

Correct Answer: C**Section: (none)****Explanation****Explanation/Reference:****QUESTION 48**

A company is preparing to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database. The database cannot be migrated to a different engine because SQL Server features are used in the application's .NET code. The company wants to attain the greatest availability possible while minimizing operational and management overhead.

What should a solutions architect do to accomplish this?

- A. Install SQL Server on Amazon C2 in a Multi-AZ deployment.
- B. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment.
- C. Deploy the database on Amazon RDS for SQL Server with Multi-AZ Replicas.
- D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment

Correct Answer: B**Section: (none)****Explanation****Explanation/Reference:****QUESTION 49**

A company is using Site-Site VPN connection for secure connectivity to its AWS cloud resource from on premises. Due to an increase in traffic across the VPN connections to the Amazon EC2 instances, users are experiencing slower VPN connectivity.

Which solution will improve the VPN throughput?

- A. Implement multiple customer gateways for the same network to scale the throughput
- B. Use a Transit Gateway with equal cost multipath routing and add additional VPN tunnels.
- C. Configure a virtual gateway with equal cost multipath routing and multiple cahnnels.
- D. Increase the number of tunnels in the VPN configuration to scale the throughput beyond the defaultlimit.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

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

What should a solution architect recommend to decouple the system?

- A. Use Amazon Kinesis Data streams to capture the data and store the JSON object in Amazon S3.
- B. Use Amazon Kinesis Data Firehouse to capture the data and store the JSON object in Amzon S3
- C. Use Amazon simple Queue service (Amzon SQS) FIFO queue to captur the data and EC2 instances toprocess the messages in the queue.
- D. Use Amazon simple Notification Service (Amazon SNS) to capture the data and EC2 instances toprocess the messages sent to Application Load balancer.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

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

What should a solutions architect recommend to accomplish this?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

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

Which managed service should a solution architect recommend?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

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

Which combination of steps should the solutions architect take? (Select TWO)

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

A company is planning to transfer multiple terabytes of data to AWS. The data is collected offline from ships. The company wants to run complex transformations before transferring the data.

Which AWS service should a solutions architect recommend for this migrations?

- A. AWS Snowball.
- B. AWS Snowmobile.
- C. AWS Snowball Edge Storage Optimized.
- D. AWS Snowball Edge Compute Optimized.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains over 10 million rows. The database has 2 TB of General Purpose SSD (gp2) storage. There are millions of updates against this data every day through the company's website. The company has noticed some operations are taking 10 seconds or longer, and has determined that the database storage performance is bottleneck.

Which solution addresses the performance issues?

- A. Change the storage type to Provisioned IOPS SSD (io1).
- B. Change the instance to a memory-optimized instance class.
- C. Change the instance to a burstable performance DB instance class.
- D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

A company has a hybrid application hosted on multiple on-premises servers with static IP addresses. There is already a VPN that provides connectivity between the VPC and the on-premises network. The company wants to distribute TCP traffic across the on-premises servers for internet users.

What should a solution architect recommend to provide a highly available and scalable solution?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

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

Which storage solution is MOST cost effective?

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Exam G

QUESTION 1

An online shopping application accesses an Amazon RDS Multi-AZ DB instance. Database performance is slowing down the application. After upgrading to the next generation instance type, there was no significant performance improvement.

Analysis shows approximately 700 IOPS are sustained, common queries run for long durations, and memory utilization is high.

Which application change should a solution architect recommend to resolve these issue?

- A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.
- B. Separate the long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database only if needed.
- C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query whichever database only if needed.
- D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

A company hosts its web application on AWS using Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

Which policy should be used to meet this requirement?

- A. Simple routing policy.
- B. Latency routing policy.
- C. Multivalue routing policy.
- D. Geolocation routing policy.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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

Which solution meets these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Key must be rotated every year.

Which solution meets these requirements and is the MOST operationally efficient?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migrations must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.

What should a solutions architect do to migrate and store the data at the LOWEST cost?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 6**

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

Which solution meets these requirements?

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

Correct Answer: B**Section: (none)****Explanation****Explanation/Reference:****QUESTION 7**

A application running on an Amazon EC2 instance needs to securely access files on an Amazon Elastic File System (Amazon EFS) file system. The EFS files are stored using encryption at rest.

Which solution for accessing the files is MOST secure?

- A. Enable TLS when mounting Amazon EFS.
- B. Store the encryption key in the code of the application.
- C. Enable AWS Key Management Service (AKS KMS) when mounting Amazon EFS.
- D. Store the encryption key in an Amazon S3 bucket and use IAM roles to grant the EC2 instance access permission.

Correct Answer: C**Section: (none)****Explanation****Explanation/Reference:****QUESTION 8**

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

Which solution meets these requirements?

- A. Set up AWS Auto Scaling to scale out the ECS service when there are timeouts on the ALB. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- B. Set up AWS Auto Scaling to scale out the ECS service when the ALB CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

- C. Set up AWS Auto Scaling to scale out the ECS service when the service's CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- D. Set up AWS Auto Scaling to scale out the ECS service when the ALB target group CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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

What should a solutions architect do to correct this issue?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A company is developing a video conversion application hosted on AWS. The application will be available in two tiers: a free tier and paid tier. User in the paid tier will have their videos converted first, and then the free tier users will have their videos converted.

Which solution meets these requirements and is MOST cost-effective?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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

What should the solutions architect do to meet these requirements?

- A. Enable DynamoDB Accelerator (DAX) to cache the data.
- B. Enable Multi-AZ replication for the DynamoDB database.
- C. Enable DynamoDB auto scaling when creating the tables.
- D. Enable DynamoDB On-Demand capacity allocation when creating the tables.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

A company is preparing to deploy a data lake on AWS. A solutions architect must define the encryption strategy for data at rest in Amazon S3. The company's security policy states.

- Keys must be rotated every 90 days.
- Strict separation of duties between key users and key administrators must be implemented.- Auditing key usage must be possible.

What should the solutions architect recommend?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users. Which solution meets these requirements?

- A. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint
- B. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
- C. Order daily AWS Snowball devices Load the data onto the Snowball devices and return the devices toAWS each day.
- D. Submit a support ticket through the AWS Management Console Request the removal of S3 servicelimits from the account.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

A company uses Amazon Redshift for its data warehouse. The company wants to ensure high durability for its data in case of any component failure.

What should a solutions architect recommend?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content to meet the migration date, minimal changes can be made.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 Standard bucket with access to the web server.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) volume and mount it on all web servers.
- D. Configure Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volumes and mount them on all web servers.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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

Which solution meets these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

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

Which solution meets these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

A company is deploying an application in three AWS Regions using an Application Load Balancer. Amazon Route 53 will be used to distribute traffic between these Regions.

Which Route 53 configuration should a solutions architect use to provide the MOST high- performing experience?

- A. Create an A record with a latency policy.
- B. Create an A record with a geolocation policy
- C. Create a CNAME record with a failover policy.
- D. Create a CNAME record with a geoproximity policy.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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

What should the solutions architect recommend?

- A. Configure AWS Cloud Trail trails to log S3 API calls. Use AWS AppSync to process the files.
- B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
- C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.

- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3.
Invoke an AWS Lambda function to process the files.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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

Which storage service should a solutions architect recommend?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

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

What should the solutions architect do to meet these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Keywords to focus on would be highly available database - DynamoDB would be a better choice for leaderboard.

QUESTION 22

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

What should a solutions architect do to improve the security of data in transit to the web tier?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

User - NLB - EC2 (Web) + DB

QUESTION 23

A company uses Application Load Balancers (ALBs) in different AWS Regions.

The ALBs receive inconsistent traffic that can spike and drop throughout the year. The company's networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.

Which solution is the MOST scalable with minimal configuration changes?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters.

The company is not ready to fully migrate to the AWS Cloud, but it wants a failure environment on AWS in case the on-premises data center fails.

The company runs web servers that connect to external vendors. The data available on AWS and on premises must be uniform.

Which solution should a solutions architect recommend that has the LEAST amount of downtime?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

A company has two AWS accounts Production and Development.

There are code changes ready in the Development account to push to the Production account. In the alpha phase, only two senior developers on the development team need access to the Production account. In the beta phase, more developers might need access to perform testing as well.

What should a solutions architect recommend?

- A. Create two policy documents using the AWS Management Console in each account. Assign the policy to developers who need access.
- B. Create an IAM role in the Development account. Give one IAM role access to the Production account. Allow developers to assume the role.
- C. Create an IAM role in the Production account with the trust policy that specifies the Development account.
Allow developers to assume the role.
- D. Create an IAM group in the Production account and add it as a principal in the trust policy that specifies the Production account. Add developers to the group.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys.
Configure the application to load the database credentials from AWS KMS.
Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials inAWS Secrets Manager.
Configure the application to load the database credentials from Secrets Manager.
Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials inAWS Secrets Manager.
Configure the application to load the database credentials from Secrets Manager.
Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials inAWS Systems Manager Parameter.
Store Configure the application to load the database credentials from Parameter Store.
Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27 A web application must persist order data to Amazon S3 to support near-real-time processing.

A solutions architect needs create an architecture that is both scalable and fault tolerant.

Which solutions meet these requirements? (Select TWO.)

- A. Write the order event to an Amazon DynamoDB table.
Use DynamoDB Streams to trigger an AWS Lambda function that parses the payload and writes the data to Amazon
- B. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue.
Use the queue to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- C. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic.
Use the SNS topic to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- D. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue.
Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- E. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic.
Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service Customer Master Keys (AWS KMS CMKs).

A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Select TWO.)

- A. Attach the kms.decrypt permission to the Lambda function's resource policy.
- B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy.
- C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
- D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.
- E. Create a new IAM role with the kms decrypt permission and attach the execution role to the Lambda function.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

A company is building a document storage application on AWS. The application runs on Amazon EC2 instances in multiple Availability Zones. The company requires the document store to be highly available. The documents need to be returned immediately when requested.

The lead engineer has configured the application to use Amazon Elastic Block Store (Amazon EBS) to store the documents, but is willing to consider other options to meet the availability requirement.

What should a solutions architect recommend?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost.

The company's data science team wants to query ingested data near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

- A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

A company has a website deployed on AWS. The database backend is hosted on Amazon RDS for MySQL with a primary instance and five read replicas to support scaling needs. The read replicas should lag no more than 1 second behind the primary instance to support the user experience.

As traffic on the website continues to increase, the replicas are falling further behind during periods of peak load, resulting in complaints from users when searches yield inconsistent results.

A solutions architect needs to reduce the replication lag as much as possible, with minimal changes to the application code or operational requirements.

Which solution meets these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

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

The company follows least-privilege access rules.

```
  "Version": "2012-10-17",
  "Statement": [
```

```
    "Action": [
      "s3>ListBucket"
```

```
      "s3>DeleteObject"
```

```
    ],
    "Resource": [
```

"arn:aws:s3::

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

"Effect": "Allow"

A.

"Action": [
 "s3:*Object"
],
"Resource": [
 "arn:aws:s3:::bucketname"]

```
    ],
    "Effect": "Allow"

  },
  "Action": [
    "s3:*"
  ],
  "Resource": [
    "arn:aws:s3:::bucket"
  ],
  "Effect": "Allow"
```

C.

```
    "Action": [
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::bucketname/*"
    ],
    "Effect": "Allow"
}

{
    "Action": [
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::bucketname/*"
    ],
    "Effect": "Allow"
}
```

D.



Correct Answer: B



Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels.

The company has been experiencing application interruptions several times each day, resulting in lost transactions.

What should a solutions architect recommend to improve application resiliency?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34 A user has underutilized on-premises resources.

Which AWS Cloud concept can BEST address this issue?

- A. High Availability
- B. Elasticity
- C. Security
- D. Loose Coupling

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

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

Which design should a solutions architect recommend?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

An application is running on an Amazon EC2 instance and must have millisecond latency when running the workload. The application makes many small reads and writes to the file system, but the file system itself is small.

Which Amazon Elastic Block Store (Amazon EBS) volume type should a solutions architect attach to their EC2 instance?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

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

What should a solutions architect recommend to meet these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

A company has a media catalog with metadata for each item in the catalog. Different types of metadata are extracted from the media items by an application running on AWS Lambda. Metadata is extracted according to a number of rules, with the output stored in an Amazon ElastiCache for Redis cluster. The extraction process is done in batches and takes around 40 minutes to complete. The update process is triggered manually whenever the metadata extraction rules change.

The company wants to reduce the amount of time it takes to extract metadata from its media catalog. To achieve this, a solutions architect has split the single metadata extraction Lambda function into a Lambda function for each type of metadata.

Which additional steps should the solutions architect take to meet the requirements?

- A. Create an AWS Step Functions workflow to run the Lambda functions in parallel.
Create another Step Functions workflow that retrieves a list of media items and executes a metadata extraction workflow for each one.
- B. Create an AWS Batch compute environment for each Lambda function.
Configure an AWS Batch job queue for the compute environment.
Create a Lambda function to retrieve a list of media items and write each item to the job queue.
- C. Create an AWS Step Functions workflow to run the Lambda functions in parallel.
Create a Lambda function to retrieve a list of media items and write each item to an Amazon SQS queue. Configure the SQS queue as an input to the Step Functions workflow.
- D. Create a Lambda function to retrieve a list of media items and write each item to an Amazon SQS queue.
Subscribe the metadata extraction Lambda functions to the SQS queue with a large batch size.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

A company is deploying a public-facing global application on AWS using Amazon CloudFront. The application communicates with an external system. A solutions architect needs to ensure the data is secured during end-to-end transit and at rest.

Which combination of steps will satisfy these requirements? (Select TWO)

- A. Create a public certificate for the required domain in AWS Certificate Manager and deploy it to CloudFront, an Application Load Balancer, and Amazon EC2 instances.
- B. Acquire a public certificate from a third-party vendor and deploy it to CloudFront, an Application Load Balancer, and Amazon EC2 instances.
- C. Provision Amazon EBS encrypted volumes using AWS KMS and ensure explicit encryption of data when writing to Amazon EBS.
- D. Use SSL or encrypt data while communicating with the external system using a VPN.
- E. Communicate with the external system using plaintext and use the VPN to encrypt the data in transit.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

A company's lease of a co-located storage facility will expire in 90 days. The company wants to move to AWS to avoid signing a contract extension. The company's environment consists of 200 virtual machines and a NAS with 40 TB of data. Most of the data is archival, yet instant access is required when data is requested.

Leadership wants to ensure minimal downtime during the migration. Each virtual machine has a number of customized configurations. The company's existing 1 Gbps network connection is mostly idle, especially after business hours.

Which combination of steps should the company take to migrate to AWS while minimizing downtime and operational impact? (Select TWO.)

- A. Use new Amazon EC2 instances and reinstall all application code.
- B. Use AWS SMS to migrate the virtual machines.
- C. Use AWS Storage Gateway to migrate the data to cloud-native storage.
- D. Use AWS Snowball to migrate the data.
- E. Use AWS SMS to copy the infrequently accessed data from the NAS.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

A company is planning a large event where a promotional offer will be introduced. The company's website is hosted on AWS and backed by an Amazon RDS for PostgreSQL DB instance. The website explains the promotion and includes a sign-up page that collects user information and preferences. Management expects large and unpredictable volumes of traffic periodically, which will create many database writes.

A solutions architect needs to build a solution that does not change the underlying data model and ensures that submissions are not dropped before they are committed to the database.

Which solutions meets these requirements?

- A. Immediately before the event, scale up the existing DB instance to meet the anticipated demand. Then scale down after the event.
- B. Use Amazon SQS to decouple the application and database layers.
Configure an AWS Lambda function to write items from the queue into the database.
- C. Migrate to Amazon DynamoDB and manage throughput capacity with automatic scaling.
- D. Use Amazon ElastiCache for Memcached to increase write capacity to the DB instance.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

A solutions architect is designing a publicly accessible web application that is on an Amazon CloudFront distribution with an Amazon S3 website endpoint as the origin.

When the solution is deployed, the website returns an Error 403: Access Denied message.

Which steps should the solutions architect take to correct the issue? (Select TWO.)

- A. Remove the S3 block public access option from the S3 bucket.
- B. Remove the requester pays option from the S3 bucket.
- C. Remove the origin access identity (OAI) from the CloudFront distribution.
- D. Change the storage class from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone- IA).
- E. Disable S3 object versioning

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

A company is running a media store across multiple Amazon EC2 instances distributed across multiple Availability Zones in a single VPC.

The company wants a high-performing solution to share data between all the EC2 instances, and prefers to keep the data within the VPC only.

What should a solutions architect recommend?

- A. Create an Amazon S3 bucket and call the service APIs from each instance's application.
- B. Create an Amazon S3 bucket and configure all instances to access it as a mounted volume.
- C. Configure an Amazon Elastic Block Store (Amazon EBS) volume and mount it across all instances.
- D. Configure an Amazon Elastic File System (Amazon EFS) file system and mount it across all instances.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

A company has a 143 TB MySQL database that it wants to migrate to AWS. The plan is to use Amazon Aurora MySQL as the platform going forward. The company has a 100 Mbps AWS Direct Connect connection to Amazon VPC.

Which solution meets the company's needs and takes the LEAST amount of time?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real time recommendations. The application has a fleet of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance.

Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure.

The solution must ensure that data analysts are writing SQL to analyze the data only. No data can be lost during the deployment.

What should a solutions architect recommend?

- A. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.
- B. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.
- D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

- A. Add a set of VPNs between the Management and Production VPCs.
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

A solutions architect is designing a solution that involves orchestrating a series of Amazon Elastic Container Service (Amazon ECS) task types running on Amazon EC2 instances that are part of an ECS cluster. The output and state data for all tasks needs to be stored.

The amount of data output by each task is approximately 10MB, and there could be hundreds of tasks running at a time. The system should be optimized for high-frequency reading and writing. As old outputs are archived and deleted, the storage size is not expected to exceed 1TB.

Which storage solution should the solutions architect recommend?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

A company has three VPCs named Development, Testing, and Production in the us-east-1 Region. The three VPCs need to be connected to and on-premises data center and are designed to be separate to maintain security and prevent any resource sharing.

A solution architect needs to find a scalable and secure solution.

What should the solution architect recommend?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications.

What should a solutions architect do to reduce the operational burden?

- A. Use multi-factor authentication (MFA) to protect the encryption keys
- B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys
- C. Use AWS Certificate Manager (ACM) to create, store and assign the encryption keys
- D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys

Correct Answer: B

Section: (none)**Explanation****Explanation/Reference:****QUESTION 50**

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

How should a solutions architect provide access to the SQS queue?

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

Correct Answer: C**Section: (none)****Explanation****Explanation/Reference:****QUESTION 51**

A disaster response team is using drones to collect images from recent storm damage. The response team's laptops lack the storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.

What should a solutions architect recommend?

- A. Use AWS Snowball Edge devices to process and store the images.
- B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
- C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images.
- D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

Correct Answer: A**Section: (none)****Explanation****Explanation/Reference:****QUESTION 52**

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

Which solution meets these requirements?

- A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data storeConfigure the DynamoDB table for provisioned capacity

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

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

What should a solutions architect recommend to resolve this issue?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

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

What should a solutions architect do to ensure these requirements are met?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO.)

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

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

A solutions architect needs to ensure that all Amazon Elastic Block Store (Amazon EBS) volumes restored from unencrypted EBS snapshots are encrypted.

What should the solutions architect do to accomplish this?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

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

How should the company securely share the database with the auditor?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**Exam H****QUESTION 1**

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

Which solution will meet these requirements?

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

Correct Answer: A**Section: (none)****Explanation****Explanation/Reference:****QUESTION 2**

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

What should a solutions architect recommend to meet these requirements?

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

Correct Answer: B**Section: (none)****Explanation****Explanation/Reference:**

QUESTION 3

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0.

Company policy requires that each resource has the least access required to still be able to perform its tasks. Which additional configuration strategy should the solution architect use to meet these requirements?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

A company runs an application on an Amazon EC2 instance backed by Amazon Elastic Block Store (Amazon EBS).

The instance needs to be available for 12 hours daily. The company wants to save costs by making the instance unavailable outside the window required for the application.

However the contents of the instance's memory must be preserved whenever the instance is unavailable. What should a solutions architect do to meet this requirement?

- A. Stop the instance outside the application's availability window. Start up the instance again when required.
- B. Hibernate the instance outside the application's availability window. Start up the instance again when required.
- C. Use Auto Scaling to scale down the instance outside the application's availability window. Scale up the instance when required.
- D. Terminate the instance outside the application's availability window.
Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol. Which AWS managed service meets these requirements?

- A. Amazon EBS
- B. Amazon EC2
- C. Amazon FSx

D. Amazon S3

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

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

Which storage solution meets these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

A company hosts its application using Amazon Elastic Container Service (Amazon ECS) and wants to ensure high availability.

The company wants to be able (o deploy updates to its application even if nodes in one Availability Zone are not accessible.

The expected request volume for the application is 100 requests per second, and each container task is able to serve at least 60 requests per second. The company set up Amazon ECS with a rolling update

deployment type with the minimum healthy percent parameter set to 50% and the maximum percent set to 100%. Which configuration of tasks and Availability Zones meets these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

A web application runs on Amazon EC2 instances behind an Application Load Balancer. The application allows users to create custom reports of historical weather data.

Generating a report can take up to 5 minutes.

These long-running requests use many of the available incoming connections, making the system unresponsive to other users.

How can a solutions architect make the system more responsive?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A company is planning to use Amazon S3 to store images uploaded by its users.

The images must be encrypted at rest in Amazon S3.

The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer.

Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively

increases capacity to minimize any performance impact on application users. Which solution will meet these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have been complaining of timeouts. The architecture uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initialize upon boot up before responding to user requests. How should a solutions architect redesign the architecture to better respond to changing traffic?

- A. Configure a Network Load Balancer with a slow start configuration.
- B. Configure AWS ElastiCache for Redis to offload direct requests to the servers. C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
- D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning.

This application runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance.

Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

A company is launching an ecommerce website on AWS.

This website is built with a three-tier architecture that includes a MySQL database.

In a Multi-AZ deployment of Amazon Aurora MySQL.

The website application must be highly available and will initially be launched in an AWS Region with three Availability Zones.

The application produces a metric that describes the load the application experiences.

Which solution meets these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

A company is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in Amazon RDS MySQL Multi-AZ DB instances.

The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks. What should a solutions architect recommend?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs 3 solution with low latency and high availability.

What should a solutions architect do to accomplish this?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: <https://aws.amazon.com/global-accelerator/faqs/>

QUESTION 17 A company has a custom application running on an Amazon EC2 instance that:

- Reads a large amount of data from Amazon S3 - Performs a multi-stage analysis.
- Writes the results to Amazon DynamoDB.

The application writes a significant number of large, temporary files during the multi-stage analysis.

The process performance depends on the temporary storage performance. What would be the fastest storage option for holding the temporary files?

- A. Multiple Amazon S3 buckets with Transfer Acceleration for storage
- B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization.
- C. Multiple Amazon EFS volumes using the Network File System version 4.1 (NFSv4.1) protocol.
- D. Multiple instance store volumes with software RAID 0

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance.

The backend application then stores the data in Amazon RDS. What should a solutions architect do to decouple the architecture and make it scalable?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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

- A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3.
Connect the on-premises application servers to the file gateway using NFS.
- B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server, and copy the application data to the EFS file system.
Then connect the on-premises application to Amazon EFS.
- C. Configure AWS Storage Gateway as a volume gateway.
Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots.
- D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic FileSystem (Amazon EFS) file system as the destination for application data transfer. Connect the on-premises application to the EFS file system.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud.

The company uses tiered storage on-premises with high high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running. Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for clusters for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://aws.amazon.com/fsx/lustre/>

Amazon FSx for Lustre makes it easy and cost effective to launch and run the world's most popular high-performance file system. Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.

QUESTION 21

A software vendor is deploying a new software-as-a-service (SaaS) solution that will be utilized by many AWS users.

The service is hosted in a VPC behind a Network Load Balancer. The software vendor wants to provide access to this service to users with the least amount of administrative overhead and without exposing the service to the public internet. What should a solutions architect do to accomplish this goal?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team 1AM user credentials according to the principle of least privilege.

Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

- A. Enable the versioning and MFA Delete features on the S3 bucket
- B. Enable multi-factor authentication (MFA) on the 1AM user credentials for each audit team 1AM user account.
- C. Add an S3 Lifecycle policy to the audit team's 1AM user accounts to deny the s3:DeleteObject action during audit dates.

- D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

A solutions architect is helping a developer design a new ecommerce shopping cart application using AWS services.

The developer is unsure of the current database schema and expects to make changes as the ecommerce site grows.

The solution needs to be highly resilient and capable of automatically scaling read and write capacity. Which database solution meets these requirements?

- A. Amazon Aurora PostgreSQL
- B. Amazon DynamoDB with on-demand enabled
- C. Amazon DynamoDB with DynamoDB Streams enabled
- D. Amazon SQS and Amazon Aurora PostgreSQL

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

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

- A. Use an AWS Storage Gateway file gateway to provide file storage to AWS. Then perform analytics on the data in the AWS Cloud.
- B. Use an AWS Storage Gateway tape gateway to copy the backup of the local data to AWS. Then perform analytics on this data in the AWS Cloud.

- C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly takesnapshots of the local data, then copy the data to AWS.
- D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all thelocal storage in the AWS Cloud, then perform analytics on this data in the cloud.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

QUESTION 26

A solutions architect is designing a solution that requires frequent updates to a website that is hosted on Amazon S3 with versioning enabled.

For compliance reasons, older versions of the objects will not be accessed frequently and will need to be deleted after 2 years.

What should the solutions architect recommend to meet these requirements at the LOWEST cost?

- A. Use S3 batch operations to replace object tags.Expire the objects based on the modified tags
- B. Configure an S3 Lifecycle policy to transition older versions of objects to S3 Glacier.Expire the objects after 2 years
- C. Enable S3 Event Notifications on the bucket that sends older objects to the Amazon Simple QueueService (Amazon SOS) queue for further processing.
- D. Replicate older object versions to a new bucket.
Use an S3 Lifecycle policy to expire the objects In the new bucket after 2 years

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

A company receives 10 TB of instrumentation data each day from several machines located at a single factory.

The data consists of JSON files stored on a storage area network (SAN) in an on- premises data center located within the factory.

The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive. Which solution offers the MOST reliable data transfer?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

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

Which configuration will meet this requirement?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: <https://aws.amazon.com/es/blogs/security/how-to-use-aws-waf-to-filter-incoming-traffic-from-embargoedcountries/>

QUESTION 29

A leasing company generates and emails POF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.

What is the MOST cost-effective storage solution for this situation?

- A. Store the statements using the Amazon S3 Standard storage class.
Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
- B. Store the statements using the Amazon S3 Glacier storage class.
Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
- C. Store the statements using the Amazon S3 Standard storage class.
Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
- D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class.
Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month.

Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity.

Which solution will meet these requirements?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch.

However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

A solutions architect must design a database solution for a high-traffic ecommerce web application. The database stores customer profiles and shopping cart information. The database must support a peak load of several million requests each second and deliver responses in milliseconds.

The operational overhead for managing and scaling the database must be minimized. Which database solution should the solutions architect recommend?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

A company wants a storage option that enables its data science team to analyze its data on premises and in the AWS Cloud.

The team needs to be able to run statistical analyses by using the data on premises and by using a fleet of Amazon EC2 instances across multiple Availability Zones. What should a solutions architect do to meet these requirements?

- A. Use an AWS Storage Gateway tape gateway to copy the on-premises files into Amazon S3.
- B. Use an AWS Storage Gateway volume gateway to copy the on-premises files into Amazon S3.
- C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store(Amazon EBS).

- D. Attach an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers. Copy the files to Amazon EFS.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

A company is planning on deploying a newly built application on AWS in a default VPC. The application will consist of a web layer and database layer. The web server was created in public subnets, and the MySQL database was created in private subnets. All subnets are created with the default network ACL settings, and the default security group in the VPC will be replaced with new custom security groups. The following are the key requirements:

- The web servers must be accessible only to users on an SSL connection.
- The database should be accessible to the web layer, which is created in a public subnet only. - All traffic to and from the IP range 182.20.0.0/16 subnet should be blocked.

Which combination of steps meets these requirements? (Select TWO.)

- A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0.0.0.0/0)
- B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.
- C. Create a web server security group with an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182.20.0.0/16.
- D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0).
Create network ACL inbound and outbound deny rules for IP range 182.20.0.0/16
- E. Create a web server security group with inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0).
Create a network ACL inbound deny rule for IP range 182.20.0.0/16.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for 1AM user passwords.

What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account.
- B. Set a password policy for each 1AM user in the AWS account.
- C. Use third-party vendor software to set password requirements,

- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestType": "Create"
                }
            }
        }
    ]
}
```

```
    "ec2:Region": "us-east-1",
    "Effect": "Deny",
    "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
    ],
    "Resource": "*",
    "Condition": {
        "BoolCondition": {"aws:Requester": "not-equal", "Value": "AWSIdentityProvider"}
```

What are the effective IAM permissions of this policy for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after The Allow permission are not applied
- B. Group member are denied any Amazon EC2 permissions in the us-east-1 Region unless they are tagged in with multi-factor authentication (MFA).
- C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for allRegions when logged in with multi-factor authentication (MFA). Group members authorized any other Amazon EC2 action.
- D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Groups are permitted any other Amazon EC2 action within the us-east-1 Region

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources.

A solutions architect wants the deployment engineer to perform job activities. While following the principle of least privilege.

Which combination of actions should the solutions architect take to accomplish this goal? (Select TWO.)

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

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

A solutions architect is working on optimizing a legacy document management application running on Microsoft a network file share.

The chief information officer wants to reduce the on-premises data center footprint and minimize storage by moving on-premises storage to AWS.

What should the solution architect do to meet these requirements?

- A. Set up an AWS Storage Gateway file gateway.
- B. Set up Amazon Elastic File System (Amazon EFS).
- C. Set up AWS Storage Gateway as a volume gateway.
- D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

A company wants to migrate its web application to AWS. The legacy web application consists of a web tier, an application tier, and a MySQL database.

The re-architected application must consist of technologies that do not require the administration team to manage instances or clusters.

Which combination of services should a solutions architect include in the overall architecture? (Select TWO)

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

Correct Answer: DE

Section: (none)

Explanation**Explanation/Reference:****QUESTION 44**

A company has multiple applications that use Amazon RDS for MySQL as its database. The company recently discovered that a new custom reporting application has increased the number of queries on the database.

This is slowing down performance.

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

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

Correct Answer: D**Section: (none)****Explanation****Explanation/Reference:****QUESTION 45**

A company owns an asynchronous API that is used to ingest user requests and, based on the request type, dispatch requests to the appropriate microservice for processing. The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices.

The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests. What should a solutions architect do to address this issue without impacting existing users?

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

Correct Answer: B**Section: (none)****Explanation****Explanation/Reference:****QUESTION 46**

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation instance with 2,000 GB of storage in an Amazon EBS General Purpose SSD (gp2) volume.

The database performance impacts the application during periods of high demand.

After analyzing the logs in Amazon CloudWatch Logs, a database administrator finds that the application performance always degrades when the number of read and write IOPS is higher than 6,000. What should a solutions architect do to improve the application performance?

- A. Replace the volume with a Magnetic volume
- B. Increase the number of IOPS on the gp2 volume
- C. Replace the volume with a Provisioned IOPS (PIOPS) volume.

- D. Replace the 2,000 GB gp2 volume with two 1,000 GBgp2 volumes.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

A company is using AWS Organizations with two AWS accounts: Logistics and Sales. The Logistics account operates an Amazon Redshift cluster. The Sales account includes Amazon EC2 instances. The Sales account needs to access the Logistics account's Amazon Redshift cluster.

What should a solutions architect recommend to meet this requirement MOST cost-effectively?

- A. Set up VPC sharing with the Logistics account as the owner and the Sales account as the participant to transfer the data.
- B. Create an AWS Lambda function in the Logistics account to transfer data to the Amazon EC2 instances in the Sales account.
- C. Create a snapshot of the Amazon Redshift cluster, and share the snapshot with the Sales account. In the Sales account, restore the cluster by using the snapshot ID that is shared by the Logistics account.
- D. Run COPY commands to load data from Amazon Redshift into Amazon S3 buckets in the Logistics account. Grant permissions to the Sales account to access the S3 buckets of the Logistics account.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html>

QUESTION 48

A company is using Amazon Redshift for analytics and to generate customer reports. The company recently acquired 50 TB of additional customer demographic data. The data is stored in .csv files in Amazon S3. The company needs a solution that joins the data and visualizes the results with the least possible cost and effort.

What should a solutions architect recommend to meet these requirements?

- A. Use Amazon Redshift Spectrum to query the data in Amazon S3 directly and join that data with the existing data in Amazon Redshift. Use Amazon QuickSight to build the visualizations.
- B. Use Amazon Athena to query the data in Amazon S3. Use Amazon QuickSight to join the data from Athena with the existing data in Amazon Redshift and to build the visualizations.
- C. Increase the size of the Amazon Redshift cluster, and load the data from Amazon S3. Use Amazon EMR Notebooks to query the data and build the visualizations in Amazon Redshift.
- D. Export the data from the Amazon Redshift cluster into Apache Parquet files in Amazon S3. Use Amazon Elasticsearch Service (Amazon ES) to query the data. Use Kibana to visualize the results.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

A solutions architect must provide a fully managed replacement for an on-premises solution that allows employees and partners to exchange files. The solution must be easily accessible to employees connecting from on-premises systems, remote employees, and external partners. Which solution meets these requirements?

- A. Use AWS Transfer for SFTP to transfer files into and out of Amazon S3.
- B. Use AWS Snowball Edge for local storage and large-scale data transfers.
- C. Use Amazon FSx to store and transfer files to make them available remotely.
- D. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/aws-transfer-family/?whats-new-cards.sortby=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

QUESTION 50

A company's database is hosted on an Amazon Aurora MySQL DB cluster in the us-east-1 Region. The database is 4 TB in size. The company needs to expand its disaster recovery strategy to the us-west-2 Region. The company must have the ability to fail over to us-west-2 with a recovery time objective (RTO) of 15 minutes.

What should a solutions architect recommend to meet these requirements?

- A. Create a Multi-Region Aurora MySQL DB cluster in us-east-1 and us-west-2. Use an Amazon Route53 health check to monitor us-east-1 and fail over to us-west-2 upon failure.
- B. Take a snapshot of the DB cluster in us-east-1. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to copy the snapshot to us-west-2 and restore the snapshot in us-west-2 when failure is detected.
- C. Create an AWS CloudFormation script to create another Aurora MySQL DB cluster in us-west-2 in case of failure. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to deploy the AWS CloudFormation stack in us-west-2 when failure is detected.
- D. Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to promote the DB cluster in us-west-2 when failure is detected.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

A company is migrating its applications to AWS. Currently, applications that run on premises generate hundreds of terabytes of data that is stored on a shared file system. The company is running an analytics application in the cloud that runs hourly to generate insights from this data.

The company needs a solution to handle the ongoing data transfer between the on-premises shared file system and Amazon S3. The solution also must be able to handle occasional interruptions in internet connectivity.

Which solutions should the company use for the data transfer to meet these requirements?

- A. AWS DataSync

- B. AWS Migration Hub
- C. AWS Snowball Edge Storage Optimized
- D. AWS Transfer for SFTP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/cloud-data-migration/>

QUESTION 52

A solutions architect is designing the architecture for a new web application. The application will run on AWS Fargate containers with an Application Load Balancer (ALB) and an Amazon Aurora PostgreSQL database. The web application will perform primarily read queries against the database.

What should the solutions architect do to ensure that the website can scale with increasing traffic? (Choose two.)

- A. Enable auto scaling on the ALB to scale the load balancer horizontally.
- B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.
- C. Enable cross-zone load balancing on the ALB to distribute the load evenly across containers in all Availability Zones.
- D. Configure an Amazon Elastic Container Service (Amazon ECS) cluster in each Availability Zone to distribute the load across multiple Availability Zones.
- E. Configure Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling with a target tracking scaling policy that is based on CPU utilization.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

A company captures ordered clickstream data from multiple websites and uses batch processing to analyze the data. The company receives 100 million event records, all approximately 1 KB in size, each day. The company loads the data into Amazon Redshift each night, and business analysts consume the data. The company wants to move toward near-real-time data processing for timely insights. The solution should process the streaming data while requiring the least possible operational overhead.

Which combination of AWS services will meet these requirements MOST cost-effectively? (Choose two.)

- A. Amazon EC2
- B. AWS Batch
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

A company has a customer relationship management (CRM) application that stores data in an Amazon RDS DB instance that runs Microsoft SQL Server. They napmoc's IT staff has administrative access to the database. The database contains sensitive data. The company wants to ensure that the data is not accessible to the IT staff and that only authorized personnel can view the data. What should a solutions architect do to secure the data?

- A. Use client-side encryption with an Amazon RDS managed key.
- B. Use client-side encryption with an AWS Key Management Service (AWS KMS) customer managed key.
- C. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) default encryption key.
- D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

A company with a single AWS account runs its internet-facing containerized web application on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.

The EKS cluster is placed in a private subnet of a VPC. System administrators access the EKS cluster through a bastion host on a public subnet.

A new corporate security policy requires the company to avoid the use of bastion hosts. The company also must not allow internet connectivity to the EKS cluster.

Which solution meets these requirements MOST cost-effectively?

- A. Set up an AWS Direct Connect connection.
- B. Create a transit gateway.
- C. Establish a VPN connection.
- D. Use AWS Storage Gateway.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.

The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.

What should a solutions architect do to improve the performance of the data tier?

- A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
- B. Migrate from Amazon RDS to Amazon Elasticsearch Service (Amazon ES) with Kibana.
- C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.
- D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

Correct Answer: C

Section: (none)**Explanation****Explanation/Reference:****QUESTION 57**

A company is migrating a large, mission-critical database to AWS. A solutions architect has decided to use an Amazon RDS for MySQL Multi-AZ DB instance that is deployed with 80,000 Provisioned IOPS for storage. The solutions architect is using AWS Database Migration Service (AWS DMS) to perform the data migration. The migration is taking longer than expected, and the company wants to speed up the process.

ynapmoc ehT's network team has ruled out bandwidth as a limiting factor.

Which actions should the solutions architect take to speed up the migration? (Choose two.)

- A. Disable Multi-AZ on the target DB instance.
- B. Create a new DMS instance that has a larger instance size.
- C. Turn off logging on the target DB instance until the initial load is complete.
- D. Restart the DMS task on a new DMS instance with transfer acceleration enabled.
- E. Change the storage type on the target DB instance to Amazon Elastic Block Store (Amazon EBS)General Purpose SSD (gp2).

Correct Answer: CD**Section: (none)****Explanation****Explanation/Reference:**



CERTIFICATIONS



We provide the latest IT certification practice exams in a variety of formats and for all types of IT professionals. Our commitment to get you certified in the shortest and easiest way is evident in the quality of our products.

Our state-of-the-art Test Engine Software simulates the real exam environment and are available for: **Windows (.EXE)**, **Android App (.APK)** and **eReader (eBook)** formats. These questions and answers will help you pass your certification exam on your first try or we refund your MONEY in full.



Xcerts Certifications
Sales@Xcerts.com | <http://Xcerts.com>

Amazon

CLF-C01

AWS Certified Cloud

Practitioner Exam

QUESTION: 1

Under the shared responsibility model, which of the following is the customer responsible for?

- A. Ensuring that disk drives are wiped after use.
- B. Ensuring that firmware is updated on hardware devices.
- C. Ensuring that data is encrypted at rest.
- D. Ensuring that network cables are category six or higher.

Answer(s): C

Reference:

<https://www.whizlabs.com/blog/aws-security-shared-responsibility/>

Explanation:

AWS for a self-hosted database that requires a nightly shutdown for maintenance and cost-saving purposes

QUESTION: 2

The use of what AWS feature or service allows companies to track and categorize spending on a detailed level?

- A. Cost allocation tags
- B. Consolidated billing
- C. AWS Budgets
- D. AWS Marketplace

Answer(s): C

Reference:

<https://aws.amazon.com/blogs/startups/how-to-set-aws-budget-when-paying-with-aws-credits/>

QUESTION: 3

Which service stores objects, provides real-time access to those objects, and offers versioning and lifecycle capabilities?

- A. Amazon Glacier
- B. AWS Storage Gateway
- C. Amazon S3
- D. Amazon EBS

Answer(s): C

Reference:

<https://aws.amazon.com/s3/faqs/>

QUESTION: 4

What AWS team assists customers with accelerating cloud adoption through paid engagements in any of several specialty practice areas?

- A. AWS Enterprise Support
- B. AWS Solutions Architects
- C. AWS Professional Services
- D. AWS Account Managers

Answer(s): C

Reference:

<https://aws.amazon.com/professional-services/>

QUESTION: 5

A customer would like to design and build a new workload on AWS Cloud but does not have the AWS-related software technical expertise in-house.

Which of the following AWS programs can a customer take advantage of to achieve that outcome?

- A. AWS Partner Network Technology Partners
- B. AWS Marketplace
- C. AWS Partner Network Consulting Partners
- D. AWS Service Catalog

Answer(s): C

QUESTION: 6

Distributing workloads across multiple Availability Zones supports which cloud architecture design principle?

- A. Implement automation.
- B. Design for agility.
- C. Design for failure.
- D. Implement elasticity.

Answer(s): C

QUESTION: 7

Which AWS services can host a Microsoft SQL Server database? (Choose two.)

- A. Amazon EC2
- B. Amazon Relational Database Service (Amazon RDS)
- C. Amazon Aurora
- D. Amazon Redshift
- E. Amazon S3

Answer(s): A, B

Reference:

<https://aws.amazon.com/sql/>

QUESTION: 8

Which of the following inspects AWS environments to find opportunities that can save money for users and also improve system performance?

- A. AWS Cost Explorer
- B. AWS Trusted Advisor
- C. Consolidated billing
- D. Detailed billing

Answer(s): B

QUESTION: 9

Which of the following Amazon EC2 pricing models allow customers to use existing server-bound software licenses?

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

Answer(s): C

Reference:

<https://aws.amazon.com/ec2/pricing/>

QUESTION: 10

Which AWS characteristics make AWS cost effective for a workload with dynamic user demand? (Choose two.)

- A. High availability
- B. Shared security model
- C. Elasticity
- D. Pay-as-you-go pricing
- E. Reliability

Answer(s): C, D

QUESTION: 11

Which service enables risk auditing by continuously monitoring and logging account activity, including user actions in the AWS Management Console and AWS SDKs?

- A. Amazon CloudWatch
- B. AWS CloudTrail
- C. AWS Config
- D. AWS Health

Answer(s): B

Reference:

<https://aws.amazon.com/cloudtrail/>

QUESTION: 12

Which of the following are characteristics of Amazon S3? (Choose two.)

- A. A global file system
- B. An object store
- C. A local file store
- D. A network file system
- E. A durable storage system

Answer(s): B, E

QUESTION: 13

Which services can be used across hybrid AWS Cloud architectures? (Choose two.)

- A. Amazon Route 53
- B. Virtual Private Gateway
- C. Classic Load Balancer
- D. Auto Scaling
- E. Amazon CloudWatch default metrics

Answer(s): A, B

Reference:

<https://www.stratoscale.com/blog/cloud/building-hybrid-cloud-environment-using-amazon-cloud/>

QUESTION: 14

What costs are included when comparing AWS Total Cost of Ownership (TCO) with on-premises TCO?

- A. Project management
- B. Antivirus software licensing
- C. Data center security
- D. Software development

Answer(s): C

QUESTION: 15

A company is considering using AWS for a self-hosted database that requires a nightly shutdown for maintenance and cost-saving purposes. Which service should the company use?

- A. Amazon Redshift
- B. Amazon DynamoDB
- C. Amazon Elastic Compute Cloud (Amazon EC2) with Amazon EC2 instance store
- D. Amazon EC2 with Amazon Elastic Block Store (Amazon EBS)

Answer(s): D

QUESTION: 16

Which of the following is a correct relationship between regions, Availability Zones, and edge locations?

- A. Data centers contain regions.
- B. Regions contain Availability Zones.
- C. Availability Zones contain edge locations.
- D. Edge locations contain regions.

Answer(s): B

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/#Region_Maps_and_Edge_Networks

QUESTION: 17

Which AWS tools assist with estimating costs? (Choose three.)

- A. Detailed billing report
- B. Cost allocation tags
- C. AWS Simple Monthly Calculator
- D. AWS Total Cost of Ownership (TCO) Calculator
- E. Cost Estimator

Answer(s): B, C, D

QUESTION: 18

Which of the following are advantages of AWS consolidated billing? (Choose two.)

- A. The ability to receive one bill for multiple accounts
- B. Service limits increasing by default in all accounts
- C. A fixed discount on the monthly bill

- D. Potential volume discounts, as usage in all accounts is combined
- E. The automatic extension of the master account's AWS support plan to all accounts

Answer(s): A, D

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION: 19

Which of the following Reserved Instance (RI) pricing models provides the highest average savings compared to On-Demand pricing?

- A. One-year, No Upfront, Standard RI pricing
- B. One-year, All Upfront, Convertible RI pricing
- C. Three-year, All Upfront, Standard RI pricing
- D. Three-year, No Upfront, Convertible RI pricing

Answer(s): C

Reference:

<https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/>

QUESTION: 20

Compared with costs in traditional and virtualized data centers, AWS has:

- A. greater variable costs and greater upfront costs.
- B. fixed usage costs and lower upfront costs.
- C. lower variable costs and greater upfront costs.
- D. lower variable costs and lower upfront costs.

Answer(s): D

Reference:

[https://d1.awsstatic.com/whitepapers/introduction-to-aws-cloud-economics-final.pdf \(10\)](https://d1.awsstatic.com/whitepapers/introduction-to-aws-cloud-economics-final.pdf)

QUESTION: 21

A characteristic of edge locations is that they:

- A. host Amazon EC2 instances closer to users
- B. help lower latency and improve performance for users.
- C. cache frequently changing data without reaching the origin server.
- D. refresh data changes daily.

Answer(s): C

Reference:

<https://www.edureka.co/community/600/what-is-an-edge-location-in-aws>

QUESTION: 22

Which of the following can limit Amazon Storage Service (Amazon S3) bucket access to specific users?

- A. A public and private key-pair
- B. Amazon Inspector
- C. AWS Identity and Access Management (IAM) policies
- D. Security Groups

Answer(s): C

Reference: <https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/>

QUESTION: 23

Which of the following security-related actions are available at no cost?

- A. Calling AWS Support
- B. Contacting AWS Professional Services to request a workshop
- C. Accessing forums, blogs, and whitepapers
- D. Attending AWS classes at a local university

Answer(s): C

QUESTION: 24

Which of the Reserved Instance (RI) pricing models can change the attributes of the RI as long as the exchange results in the creation of RIs of equal or greater value?

- A. Dedicated RIs
- B. Scheduled RIs
- C. Convertible RIs
- D. Standard RIs

Answer(s): C

Reference:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

QUESTION: 25

Which AWS feature will reduce the customer's total cost of ownership (TCO)?

- A. Shared responsibility security model
- B. Single tenancy
- C. Elastic computing
- D. Encryption

Answer(s): C

QUESTION: 26

Which of the following services will automatically scale with an expected increase in web traffic?

- A. AWS CodePipeline
- B. Elastic Load Balancing
- C. Amazon EBS
- D. AWS Direct Connect

Answer(s): B

Reference:

<https://aws.amazon.com/elasticloadbalancing/>

QUESTION: 27

Where are AWS compliance documents, such as an SOC 1 report, located?

- A. Amazon Inspector
- B. AWS CloudTrail
- C. AWS Artifact
- D. AWS Certificate Manager

Answer(s): C

Reference:

<https://aws.amazon.com/compliance/soc-faqs/>

QUESTION: 28

Under the AWS shared responsibility model, which of the following activities are the customer's responsibility? (Choose two.)

- A. Patching operating system components for Amazon Relational Database Server (Amazon RDS)
- B. Encrypting data on the client-side
- C. Training the data center staff
- D. Configuring Network Access Control Lists (ACL)
- E. Maintaining environmental controls within a data center

Answer(s): B, D

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 29

Which is a recommended pattern for designing a highly available architecture on AWS?

- A. Ensure that components have low-latency network connectivity.
- B. Run enough Amazon EC2 instances to operate at peak load.
- C. Ensure that the application is designed to accommodate failure of any single component.
- D. Use a monolithic application that handles all operations.

Answer(s): C

QUESTION: 30

According to best practices, how should an application be designed to run in the AWS Cloud?

- A. Use tightly coupled components.
- B. Use loosely coupled components.
- C. Use infrequently coupled components.
- D. Use frequently coupled components.

Answer(s): B

Reference:

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

QUESTION: 31

AWS supports which of the following methods to add security to Identity and Access Management (IAM) users? (Choose two.)

- A. Implementing Amazon Rekognition
- B. Using AWS Shield-protected resources
- C. Blocking access with Security Groups
- D. Using Multi-Factor Authentication (MFA)
- E. Enforcing password strength and expiration

Answer(s): D, E

QUESTION: 32

Which AWS services should be used for read/write of constantly changing data? (Choose two.)

- A. Amazon Glacier
- B. Amazon RDS
- C. AWS Snowball
- D. Amazon Redshift
- E. Amazon EFS

Answer(s): B, E

QUESTION: 33

What is one of the advantages of the Amazon Relational Database Service (Amazon RDS)?

- A. It simplifies relational database administration tasks.
- B. It provides 99.9999999999% reliability and durability.
- C. It automatically scales databases for loads.
- D. It enabled users to dynamically adjust CPU and RAM resources.

Answer(s): A

QUESTION: 34

A customer needs to run a MySQL database that easily scales. Which AWS service should they use?

- A. Amazon Aurora
- B. Amazon Redshift
- C. Amazon DynamoDB
- D. Amazon ElastiCache

Answer(s): A

Reference:

<https://aws.amazon.com/rds/aurora/serverless/>

QUESTION: 35

Which of the following components of the AWS Global Infrastructure consists of one or more discrete data centers interconnected through low latency links?

- A. Availability Zone
- B. Edge location
- C. Region
- D. Private networking

Answer(s): A

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/global-infrastructure.html>

QUESTION: 36

Which of the following is a shared control between the customer and AWS?

- A. Providing a key for Amazon S3 client-side encryption
- B. Configuration of an Amazon EC2 instance
- C. Environmental controls of physical AWS data centers
- D. Awareness and training

Answer(s): D

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 37

How many Availability Zones should compute resources be provisioned across to achieve high availability?

- A. A minimum of one
- B. A minimum of two
- C. A minimum of three
- D. A minimum of four or more

Answer(s): B

QUESTION: 38

One of the advantages to moving infrastructure from an on-premises data center to the AWS Cloud is:

- A. it allows the business to eliminate IT bills.
- B. it allows the business to put a server in each customer's data center.
- C. it allows the business to focus on business activities.
- D. it allows the business to leave servers unpatched.

Answer(s): C

QUESTION: 39

What is the lowest-cost, durable storage option for retaining database backups for immediate retrieval?

- A. Amazon S3
- B. Amazon Glacier
- C. Amazon EBS
- D. Amazon EC2 Instance Store

Answer(s): A

QUESTION: 40

Which AWS IAM feature allows developers to access AWS services through the AWS CLI?

- A. API keys
- B. Access keys
- C. User names/Passwords
- D. SSH keys

Answer(s): B

QUESTION: 41

Which of the following is a fast and reliable NoSQL database service?

- A. Amazon Redshift
- B. Amazon RDS
- C. Amazon DynamoDB
- D. Amazon S3

Answer(s): C

Reference:

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

QUESTION: 42

What is an example of agility in the AWS Cloud?

- A. Access to multiple instance types
- B. Access to managed services
- C. Using Consolidated Billing to produce one bill
- D. Decreased acquisition time for new compute resources

Answer(s): D

Reference:

<https://aws.amazon.com/blogs/enterprise-strategy/risk-is-lack-of-agility/>

QUESTION: 43

Which service should a customer use to consolidate and centrally manage multiple AWS accounts?

- A. AWS IAM
- B. AWS Organizations
- C. AWS Schema Conversion Tool
- D. AWS Config

Answer(s): B

Reference:

<https://aws.amazon.com/organizations/>

QUESTION: 44

What approach to transcoding a large number of individual video files adheres to AWS architecture principles?

- A. Using many instances in parallel

- B. Using a single large instance during off-peak hours
- C. Using dedicated hardware
- D. Using a large GPU instance type

Answer(s): A

Reference:

<https://aws.amazon.com/solutions/case-studies/encoding/>

QUESTION: 45

For which auditing process does AWS have sole responsibility?

- A. AWS IAM policies
- B. Physical security
- C. Amazon S3 bucket policies
- D. AWS CloudTrail Logs

Answer(s): B

QUESTION: 46

Which feature of the AWS Cloud will support an international company's requirement for low latency to all of its customers?

- A. Fault tolerance
- B. Global reach
- C. Pay-as-you-go pricing
- D. High availability

Answer(s): B

QUESTION: 47

Which of the following is the customer's responsibility under the AWS shared responsibility model?

- A. Patching underlying infrastructure
- B. Physical security
- C. Patching Amazon EC2 instances
- D. Patching network infrastructure

Answer(s): C

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 48

A customer is using multiple AWS accounts with separate billing.

How can the customer take advantage of volume discounts with minimal impact to the AWS resources?

- A. Create one global AWS account and move all AWS resources to the account.
- B. Sign up for three years of Reserved Instance pricing up front.
- C. Use the consolidated billing feature from AWS Organizations.
- D. Sign up for the AWS Enterprise support plan to get volume discounts.

Answer(s): C

Reference:

<https://aws.amazon.com/answers/account-management/aws-multi-account-billing-strategy/>

QUESTION: 49

Which of the following are features of Amazon CloudWatch Logs? (Choose two.)

- A. Summaries by Amazon Simple Notification Service (Amazon SNS)
- B. Free Amazon Elasticsearch Service analytics
- C. Provided at no charge
- D. Real-time monitoring
- E. Adjustable retention

Answer(s): D, E

QUESTION: 50

Which of the following is an AWS managed Domain Name System (DNS) web service?

- A. Amazon Route 53
- B. Amazon Neptune
- C. Amazon SageMaker
- D. Amazon Lightsail

Answer(s): A

Reference:

<https://aws.amazon.com/getting-started/tutorials/get-a-domain/>

QUESTION: 51

A customer is deploying a new application and needs to choose an AWS Region. Which of the following factors could influence the customer's decision? (Choose two.)

- A. Reduced latency to users
- B. The application's presentation in the local language
- C. Data sovereignty compliance
- D. Cooling costs in hotter climates
- E. Proximity to the customer's office for on-site visits

Answer(s): A, C

QUESTION: 52

Which storage service can be used as a low-cost option for hosting static websites?

- A. Amazon Glacier
- B. Amazon DynamoDB
- C. Amazon Elastic File System (Amazon EFS)
- D. Amazon Simple Storage Service (Amazon S3)

Answer(s): D

Reference:

<https://aws.amazon.com/getting-started/projects/host-static-website/>

QUESTION: 53

Which Amazon EC2 instance pricing model can provide discounts of up to 90%?

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

Answer(s): D

Reference:

<https://aws.amazon.com/ec2/spot/>

QUESTION: 54

What is the AWS customer responsible for according to the AWS shared responsibility model?

- A. Physical access controls
- B. Data encryption
- C. Secure disposal of storage devices
- D. Environmental risk management

Answer(s): B

QUESTION: 55

Which of the following AWS Cloud services can be used to run a customer-managed relational database?

- A. Amazon EC2
- B. Amazon Route 53
- C. Amazon ElastiCache

D. Amazon DynamoDB

Answer(s): A

QUESTION: 56

A company is looking for a scalable data warehouse solution.

Which of the following AWS solutions would meet the company's needs?

- A. Amazon Simple Storage Service (Amazon S3)
- B. Amazon DynamoDB
- C. Amazon Kinesis
- D. Amazon Redshift

Answer(s): D

Reference:

<https://aws.amazon.com/redshift/>

QUESTION: 57

Which statement best describes Elastic Load Balancing?

- A. It translates a domain name into an IP address using DNS.
- B. It distributes incoming application traffic across one or more Amazon EC2 instances.
- C. It collects metrics on connected Amazon EC2 instances.
- D. It automatically adjusts the number of Amazon EC2 instances to support incoming traffic.

Answer(s): B

Reference:

<https://aws.amazon.com/elasticloadbalancing/>

QUESTION: 58

Which of the following are valid ways for a customer to interact with AWS services? (Choose two.)

- A. Command line interface
- B. On-premises
- C. Software Development Kits
- D. Software-as-a-service
- E. Hybrid

Answer(s): A, C

QUESTION: 59

The AWS Cloud's multiple Regions are an example of:

- A. agility.
- B. global infrastructure.
- C. elasticity.
- D. pay-as-you-go pricing.

Answer(s): B

QUESTION: 60

Which of the following AWS services can be used to serve large amounts of online video content with the lowest possible latency? (Choose two.)

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

Answer(s): B, E

Reference:

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

<https://aws.amazon.com/cloudfront/>

QUESTION: 61

Web servers running on Amazon EC2 access a legacy application running in a corporate data center. What term would describe this model?

- A. Cloud-native
- B. Partner network
- C. Hybrid architecture
- D. Infrastructure as a service

Answer(s): C

Reference:

<https://aws.amazon.com/enterprise/hybrid/>

QUESTION: 62

What is the benefit of using AWS managed services, such as Amazon ElastiCache and Amazon Relational Database Service (Amazon RDS)?

- A. They require the customer to monitor and replace failing instances.
- B. They have better performance than customer-managed services.
- C. They simplify patching and updating underlying OSs.
- D. They do not require the customer to optimize instance type or size selections.

Answer(s): C

QUESTION: 63

Which service provides a virtually unlimited amount of online highly durable object storage?

- A. Amazon Redshift
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon Elastic Container Service (Amazon ECS)
- D. Amazon S3

Answer(s): D

Reference:

<https://aws.amazon.com/what-is-cloud-object-storage/>

QUESTION: 64

Which of the following Identity and Access Management (IAM) entities is associated with an access key ID and secret access key when using AWS Command Line Interface (AWS CLI)?

- A. IAM group
- B. IAM user
- C. IAM role
- D. IAM policy

Answer(s): B

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

QUESTION: 65

Which of the following security-related services does AWS offer? (Choose two.)

- A. Multi-factor authentication physical tokens
- B. AWS Trusted Advisor security checks
- C. Data encryption
- D. Automated penetration testing
- E. Amazon S3 copyrighted content detection

Answer(s): B, C

Reference:

<https://aws.amazon.com/security/>

QUESTION: 66

Which AWS managed service is used to host databases?

- A. AWS Batch
- B. AWS Artifact
- C. AWS Data Pipeline
- D. Amazon RDS

Answer(s): D

Explanation:

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

Reference:

<https://aws.amazon.com/rds/?c=db&sec=srv>

QUESTION: 67

Which AWS service provides a simple and scalable shared file storage solution for use with Linux-based AWS and on-premises servers?

- A. Amazon S3
- B. Amazon Glacier
- C. Amazon EBS
- D. Amazon EFS

Answer(s): D

Explanation:

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

Amazon EFS is designed to provide the throughput, IOPS, and low latency needed for Linux workloads. Throughput and IOPS scale as a file system grows and can burst to higher throughput levels for short periods of time to support the unpredictable performance needs of file workloads. For the most demanding workloads, Amazon EFS can support performance over 10 GB/sec and up to 500,000 IOPS.

QUESTION: 68

When architecting cloud applications, which of the following are a key design principle?

- A. Use the largest instance possible
- B. Provision capacity for peak load

- C. Use the Scrum development process
- D. Implement elasticity

Answer(s): D

Explanation:

Cloud services main proposition is to provide elasticity through horizontal scaling. It's already there. As for using largest instance possible, it is not a design principle that helps cloud applications in anyway. Scrum development process is not related to architecting. Therefore, a key principle is to provision your application for on-demand capacity. Peak loads is something that cloud applications experience everyday. Peak load management should be a necessary part of cloud application design principle.

Reference:

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

QUESTION: 69

Which AWS service should be used for long-term, low-cost storage of data backups?

- A. Amazon RDS
- B. Amazon Glacier
- C. AWS Snowball
- D. AWS EBS

Answer(s): B

Explanation:

Amazon S3 Glacier is a secure, durable, and low-cost storage class of S3 for data archiving and long-term backup. Customers can store large or small amounts of data for as little as \$0.004 per gigabyte per month. The S3 Glacier storage class is ideal for archives where data is regularly retrieved and some of the data may be needed in minutes.

Amazon RDS is a relational database service that hosts databases. It helps you create and manage databases. Amazon Snowball is a petabyte-scale data transfer service that provides cost efficient data transfer to AWS from tamper proof physical devices. Similarly, Elastic block storage offers persistent block storage volumes for EC2 instances.

Reference:

<https://aws.amazon.com/backup-restore/services/>

QUESTION: 70

Under the shared responsibility model, which of the following is a shared control between a customer and AWS?

- A. Physical controls
- B. Patch management
- C. Zone security
- D. Data center auditing

Answer(s): B

QUESTION: 71

Which AWS service allows companies to connect an Amazon VPC to an on-premises data center?

- A. AWS VPN
- B. Amazon Redshift
- C. API Gateway
- D. Amazon Direct Connect

Answer(s): D

Explanation:

AWS Direct Connect enables you to securely connect your AWS environment to your on-premises data center or office location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic connection. AWS Direct Connect offers dedicated high speed, low latency connection, which bypasses internet service providers in your network path. An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, as well as access to other US regions. AWS Direct Connect allows you to logically partition the fiber-optic connections into multiple logical connections called Virtual Local Area Networks (VLAN). You can take advantage of these logical connections to improve security, differentiate traffic, and achieve compliance requirements.

Reference:

<https://aws.amazon.com/getting-started/projects/connect-data-center-to-aws/>

QUESTION: 72

A company wants to reduce the physical compute footprint that developers use to run code. Which service would meet that need by enabling serverless architectures?

- A. Amazon Elastic Compute Cloud (Amazon EC2)
- B. AWS Lambda
- C. Amazon DynamoDB
- D. AWS CodeCommit

Answer(s): B

Explanation:

AWS Lambda is an integral part of coding on AWS. It reduces physical compute footprint by utilizing aws cloud services to run code.

QUESTION: 73

Which AWS service provides alerts when an AWS event may impact a company's AWS resources?

- A. AWS Personal Health Dashboard
- B. AWS Service Health Dashboard
- C. AWS Trusted Advisor
- D. AWS Infrastructure Event Management

Answer(s): A

Explanation:

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

Reference:

<https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/>

QUESTION: 74

Which of the following are categories of AWS Trusted Advisor? (Choose two.)

- A. Fault Tolerance
- B. Instance Usage
- C. Infrastructure
- D. Performance
- E. Storage Capacity

Answer(s): A, D

Explanation:

Like your customized cloud expert, AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: cost optimization, performance, security, fault tolerance and service limits.

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

QUESTION: 75

Which task is AWS responsible for in the shared responsibility model for security and compliance?

- A. Granting access to individuals and services
- B. Encrypting data in transit
- C. Updating Amazon EC2 host firmware
- D. Updating operating systems

Answer(s): C

Explanation:

AWS Compliance enables customers to establish and operate in an AWS security control environment

- The shared responsibility model is part of AWS Compliance program
- The Security of the cloud is managed by Amazon AWS provider The Security in the cloud is responsibility of the customer
- The customer is responsible for their information and data, their secure transmission, integrity, and encryption
- Also, the customer is responsible for managing, support, patching and control of the guest operating system and AWS services provided like EC2
- AWS customers retain control and ownership of their data
- The AWS network provides significant protection against traditional network security issues and the customer can implement further protection

Reference:

<https://www.whizlabs.com/blog/aws-security-shared-responsibility/>

QUESTION: 76

Where should a company go to search software listings from independent software vendors to find, test, buy and deploy software that runs on AWS?

- A. AWS Marketplace
- B. Amazon Lumberyard
- C. AWS Artifact
- D. Amazon CloudSearch

Answer(s): A

Explanation:

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS.

Reference:

<https://aws.amazon.com>

QUESTION: 77

Which of the following is a benefit of using the AWS Cloud?

- A. Permissive security removes the administrative burden.
- B. Ability to focus on revenue-generating activities.
- C. Control over cloud network hardware.
- D. Choice of specific cloud hardware vendors.

Answer(s): B

Explanation:

Developer and IT staff productivity accounted for nearly 30% of overall financial benefits. The remaining benefits were driven by the flexibility and agility of Amazon cloud infrastructure services, which make it easier to trial new business models, support revenue-generating applications, and provide more reliable services to end users.

Reference:

https://media.amazonwebservices.com/IDC_Business_Value_of_AWS_Accelerates_Over_time.pdf

QUESTION: 78

When performing a cost analysis that supports physical isolation of a customer workload, which compute hosting model should be accounted for in the Total Cost of Ownership (TCO)?

- A. Dedicated Hosts
- B. Reserved Instances
- C. On-Demand Instances
- D. No Upfront Reserved Instances

Answer(s): A**Explanation:**

Use Dedicated Hosts to launch Amazon EC2 instances on physical servers that are dedicated for your use. Dedicated Hosts give you additional visibility and control over how instances are placed on a physical server, and you can reliably use the same physical server over time. As a result, Dedicated Hosts enable you to use your existing server-bound software licenses like Windows Server and address corporate compliance and regulatory requirements.

QUESTION: 79

Which AWS service provides the ability to manage infrastructure as code?

- A. AWS CodePipeline
- B. AWS CodeDeploy
- C. AWS Direct Connect
- D. AWS CloudFormation

Answer(s): D**Explanation:**

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. 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. This file serves as the single source of truth for your cloud environment.

Reference:

<https://aws.amazon.com/cloudformation/>

QUESTION: 80

If a customer needs to audit the change management of AWS resources, which of the following AWS services should the customer use?

- A. AWS Config
- B. AWS Trusted Advisor
- C. Amazon CloudWatch
- D. Amazon Inspector

Answer(s): A

Explanation:

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Reference:

<https://aws.amazon.com/config/>

QUESTION: 81

What is Amazon CloudWatch?

- A. A code repository with customizable build and team commit features.
- B. A metrics repository with customizable notification thresholds and channels.
- C. A security configuration repository with threat analytics.
- D. A rule repository of a web application firewall with automated vulnerability prevention features.

Answer(s): B

Explanation:

Amazon CloudWatch is basically a metrics repository. An AWS service — such as Amazon EC2 — puts metrics into the repository, and you retrieve statistics based on those metrics. If you put your own custom metrics into the repository, you can retrieve statistics on these metrics as well.

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_architecture.html

QUESTION: 82

Which service allows a company with multiple AWS accounts to combine its usage to obtain volume discounts?

- A. AWS Server Migration Service
- B. AWS Organizations
- C. AWS Budgets
- D. AWS Trusted Advisor

Answer(s): B

Explanation:

Use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. Every organization in AWS Organizations has a master account that pays the charges of all the member accounts.

Consolidated billing has the following benefits:

- One bill – You get one bill for multiple accounts.
- Easy tracking – You can track the charges across multiple accounts and download the combined cost and usage data.
- Combined usage – You can combine the usage across all accounts in the organization to share the volume pricing discounts and Reserved Instance discounts. This can result in a lower charge for your project, department, or company than with individual standalone accounts. For more information, see Volume Discounts.
- No extra fee – Consolidated billing is offered at no additional cost.
-

QUESTION: 83

Which of the following services could be used to deploy an application to servers running on-premises? (Choose two.)

- A. AWS Elastic Beanstalk
- B. AWS OpsWorks
- C. AWS CodeDeploy
- D. AWS Batch
- E. AWS X-Ray

Answer(s): B, C

Reference:

<https://docs.aws.amazon.com/codedeploy/latest/userguide/instances-on-premises.html>

<https://aws.amazon.com/blogs/aws/opsworks-on-prem-and-existing-instances/>

QUESTION: 84

Which Amazon EC2 pricing model adjusts based on supply and demand of EC2 instances?

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

Answer(s): C

Explanation:

In the new model, the Spot prices are more predictable, updated less frequently, and are determined by supply and demand for Amazon EC2 spare capacity, not bid prices.

Reference:

<https://aws.amazon.com/blogs/compute/new-amazon-ec2-spot-pricing/>

QUESTION: 85

Which design principles for cloud architecture are recommended when re-architecting a large monolithic application? (Choose two.)

- A. Use manual monitoring.
- B. Use fixed servers.
- C. Implement loose coupling.
- D. Rely on individual components.
- E. Design for scalability.

Answer(s): C, E

Explanation:

Rearchitecting applications involves sweeping change where an old monolithic application is completely revamped according to modern microservices architecture. Using individual components to re-architect a big application is one part of the process. The most important part is to design the application for scalability because the level of investment for a monolithic application can only be justified when resilience and scalability is needed.

Reference:

<https://www.architech.ca/re-architect-applications/>

QUESTION: 86

Which is the MINIMUM AWS Support plan that allows for one-hour target response time for support cases?

- A. Enterprise
- B. Business
- C. Developer
- D. Basic

Answer(s): B

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

QUESTION: 87

Where can AWS compliance and certification reports be downloaded?

- A. AWS Artifact
- B. AWS Concierge
- C. AWS Certificate Manager
- D. AWS Trusted Advisor

Answer(s): A

Explanation:

WS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS's security and compliance reports and select online agreements. The AWS SOC 2 report is particularly helpful for completing questionnaires because it provides a comprehensive description of the implementation and operating effectiveness of AWS security controls. Another useful document is the Executive Briefing within the AWS FedRAMP Partner Package.

Reference:

<https://aws.amazon.com/compliance/faq/>

QUESTION: 88

Which AWS service provides a customized view of the health of specific AWS services that power a customer's workloads running on AWS?

- A. AWS Service Health Dashboard
- B. AWS X-Ray
- C. AWS Personal Health Dashboard
- D. Amazon CloudWatch

Answer(s): C

Explanation:

Personal Health Dashboard gives you a personalized view of the status of the AWS services that power your applications, enabling you to quickly see when AWS is experiencing issues that may impact you. For example, in the event of a lost EBS volume associated with one of your EC2 instances, you would gain quick visibility into the status of the specific service you are using, helping save precious time troubleshooting to determine root cause.

Reference:

<https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/>

QUESTION: 89

Which of the following is an advantage of consolidated billing on AWS?

- A. Volume pricing qualification

- B. Shared access permissions
- C. Multiple bills per account
- D. Eliminates the need for tagging

Answer(s): A

Explanation:

If you have multiple standalone accounts, your charges might decrease if you add the accounts to an organization. AWS combines usage from all accounts in the organization to qualify you for volume pricing discounts.

Reference:

<https://help.nops.io/consolidated-billing>

QUESTION: 90

Which of the following steps should be taken by a customer when conducting penetration testing on AWS?

- A. Conduct penetration testing using Amazon Inspector, and then notify AWS support.
- B. Request and wait for approval from the customer's internal security team, and then conduct testing.
- C. Notify AWS support, and then conduct testing immediately.
- D. Request and wait for approval from AWS support, and then conduct testing.

Answer(s): D

Explanation:

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services.

Reference:

<https://aws.amazon.com/security/penetration-testing/>

QUESTION: 91

Which of the following AWS features enables a user to launch a pre-configured Amazon Elastic Compute Cloud (Amazon EC2) instance?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Machine Image
- C. Amazon EC2 Systems Manager
- D. Amazon AppStream 2.0

Answer(s): B

Explanation:

To use Amazon EC2, you simply:

- Select a pre-configured, templated Amazon Machine Image (AMI) to get up and running immediately. Or create an AMI containing your applications, libraries, data, and associated configuration settings.
- Configure security and network access on your Amazon EC2 instance.
- Choose which instance type(s) you want, then start, terminate, and monitor as many instances of your AMI as needed, using the web service APIs or the variety of management tools provided.
- Determine whether you want to run in multiple locations, utilize static IP endpoints, or attach persistent block storage to your instances.
- Pay only for the resources that you actually consume, like instance-hours or data transfer.

Reference:

<https://aws.amazon.com/ec2/features/>

QUESTION: 92

How would an AWS customer easily apply common access controls to a large set of users?

- Apply an IAM policy to an IAM group.
- Apply an IAM policy to an IAM role.
- Apply the same IAM policy to all IAM users with access to the same workload.
- Apply an IAM policy to an Amazon Cognito user pool.

Answer(s): A**Explanation:**

Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (administrators, developers, accounting, etc.). Next, define the relevant permissions for each group. Finally, assign IAM users to those groups. All the users in an IAM group inherit the permissions assigned to the group. That way, you can make changes for everyone in a group in just one place. As people move around in your company, you can simply change what IAM group their IAM user belongs to.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

QUESTION: 93

What technology enables compute capacity to adjust as loads change?

- Load balancing
- Automatic failover
- Round robin
- Auto Scaling

Answer(s): D

Explanation:

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas. AWS Auto Scaling makes scaling simple with recommendations that allow you to optimize performance, costs, or balance between them. If you're already using Amazon EC2 Auto Scaling to dynamically scale your Amazon EC2 instances, you can now combine it with AWS Auto Scaling to scale additional resources for other AWS services. With AWS Auto Scaling, your applications always have the right resources at the right time.

Reference:

<https://aws.amazon.com/autoscaling/>

QUESTION: 94

Which AWS services are defined as global instead of regional? (Choose two.)

- A. Amazon Route 53
- B. Amazon EC2
- C. Amazon S3
- D. Amazon CloudFront
- E. Amazon DynamoDB

Answer(s): A, D

Reference:

<http://jayendrapatil.com/aws-global-vs-regional-vs-az-resources/>

QUESTION: 95

Which AWS service would you use to obtain compliance reports and certificates?

- A. AWS Artifact
- B. AWS Lambda
- C. Amazon Inspector
- D. AWS Certificate Manager

Answer(s): A

Explanation:

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating

effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Reference:

<https://aws.amazon.com/artifact/>

QUESTION: 96

Under the shared responsibility model, which of the following tasks are the responsibility of the AWS customer? (Choose two.)

- A. Ensuring that application data is encrypted at rest
- B. Ensuring that AWS NTP servers are set to the correct time
- C. Ensuring that users have received security training in the use of AWS services
- D. Ensuring that access to data centers is restricted
- E. Ensuring that hardware is disposed of properly

Answer(s): A, C

QUESTION: 97

Which AWS service can be used to manually launch instances based on resource requirements?

- A. Amazon EBS
- B. Amazon S3
- C. Amazon EC2
- D. Amazon ECS

Answer(s): C

QUESTION: 98

A company is migrating an application that is running non-interruptible workloads for a three-year time frame. Which pricing construct would provide the MOST cost-effective solution?

- A. Amazon EC2 Spot Instances
- B. Amazon EC2 Dedicated Instances
- C. Amazon EC2 On-Demand Instances
- D. Amazon EC2 Reserved Instances

Answer(s): D

QUESTION: 99

The financial benefits of using AWS are: (Choose two.)

- A. reduced Total Cost of Ownership (TCO).
- B. increased capital expenditure (capex).

- C. reduced operational expenditure (opex).
- D. deferred payment plans for startups.
- E. business credit lines for startups

Answer(s): A, C

QUESTION: 100

Which AWS Cost Management tool allows you to view the most granular data about your AWS bill?

- A. AWS Cost Explorer
- B. AWS Budgets
- C. AWS Cost and Usage report
- D. AWS Billing dashboard

Answer(s): C

Explanation:

The Cost & Usage Report is your one-stop-shop for accessing the most granular data about your AWS costs and usage. You can also load your cost and usage information into Amazon Athena, Amazon Redshift, AWS QuickSight, or a tool of your choice.

Reference:

<https://aws.amazon.com/aws-cost-management/>

QUESTION: 101

Which of the following can an AWS customer use to launch a new Amazon Relational Database Service (Amazon RDS) cluster?

- A. AWS Concierge
- B. AWS CloudFormation
- C. Amazon Simple Storage Service (Amazon S3)
- D. Amazon EC2 Auto Scaling
- E. AWS Management Console

Answer(s): E

QUESTION: 102

Which of the following is an AWS Cloud architecture design principle?

- A. Implement single points of failure.
- B. Implement loose coupling.
- C. Implement monolithic design.
- D. Implement vertical scaling.

Answer(s): B

Explanation:

Loose coupling between services can also be done through asynchronous integration. It involves one component that generates events and another that consumes them. The two components do not integrate through direct point-to-point interaction, but usually through an intermediate durable storage layer. This approach decouples the two components and introduces additional resiliency. So, for example, if a process that is reading messages from the queue fails, messages can still be added to the queue to be processed when the system recovers.

Reference:

<https://www.botmetric.com/blog/aws-cloud-architecture-design-principles/>

QUESTION: 103

Which of the following security measures protect access to an AWS account? (Choose two.)

- A. Enable AWS CloudTrail.
- B. Grant least privilege access to IAM users.
- C. Create one IAM user and share with many developers and users.
- D. Enable Amazon CloudFront.
- E. Activate multi-factor authentication (MFA) for privileged users.

Answer(s): B, E

Explanation:

If you decided to create service accounts (that is, accounts used for programmatic access by applications running outside of the AWS environment) and generate access keys for them, you should create a dedicated service account for each use case. This will allow you to restrict the associated policy to only the permissions needed for the particular use case, limiting the blast radius if the credentials are compromised. For example, if a monitoring tool and a release management tool both require access to your AWS environment, create two separate service accounts with two separate policies that define the minimum set of permissions for each tool.

Reference:

<https://aws.amazon.com/blogs/security/guidelines-for-protecting-your-aws-account-while-using-programmatic-access/>

QUESTION: 104

Which service provides a hybrid storage service that enables on-premises applications to seamlessly use cloud storage?

- A. Amazon Glacier
- B. AWS Snowball
- C. AWS Storage Gateway
- D. Amazon Elastic Block Storage (Amazon EBS)

Answer(s): C

Explanation:

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving tape backups to the cloud, reducing on-premises storage with cloud-backed file shares, providing low latency access to data in AWS for on-premises applications, as well as various migration, archiving, processing, and disaster recovery use cases.

Reference:

<https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

QUESTION: 105

Which of the following services falls under the responsibility of the customer to maintain operating system configuration, security patching, and networking?

- A. Amazon RDS
- B. Amazon EC2
- C. Amazon ElastiCache
- D. AWS Fargate

Answer(s): B

Explanation:

The customer is responsible for managing, support, patching and control of the guest operating system and AWS services provided like EC2.

Reference:

<https://www.whizlabs.com/blog/aws-security-shared-responsibility/>

QUESTION: 106

Which of the following is an important architectural design principle when designing cloud applications?

- A. Use multiple Availability Zones.
- B. Use tightly coupled components.
- C. Use open source software.
- D. Provision extra capacity.

Answer(s): A

Explanation:

Data Center resilience is practiced through Availability Zones across data centers that reduce the impact of failures.

Fault isolation improvement can be made to traditional horizontal scaling by sharding (a method of grouping instances into groups called shards, instead of sending the traffic from all users to every node like in the traditional IT structure.)

Reference:

<https://www.botmetric.com/blog/aws-cloud-architecture-design-principles/>

QUESTION: 107

Which AWS support plan includes a dedicated Technical Account Manager?

- A. Developer
- B. Enterprise
- C. Business
- D. Basic

Answer(s): B**Explanation:**

The enterprise support plans supports technical account manager. Developer and business support plans are devoid of this facility.

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

QUESTION: 108

Amazon Relational Database Service (Amazon RDS) offers which of the following benefits over traditional database management?

- A. AWS manages the data stored in Amazon RDS tables.
- B. AWS manages the maintenance of the operating system.
- C. AWS automatically scales up instance types on demand.
- D. AWS manages the database type.

Answer(s): B**QUESTION: 109**

Which service is best for storing common database query results, which helps to alleviate database access load?

- A. Amazon Machine Learning
- B. Amazon SQS
- C. Amazon ElastiCache
- D. Amazon EC2 Instance Store

Answer(s): C

Explanation:

Amazon ElastiCache for Redis is a great choice for implementing a highly available, distributed, and secure in- memory cache to decrease access latency, increase throughput, and ease the load off your relational or NoSQL databases and applications. ElastiCache can serve frequently requested items at sub-millisecond response times, and enables you to easily scale for higher loads without growing the costlier backend databases. Database query results caching, persistent session caching, and full-page caching are all popular examples of caching with ElastiCache for Redis.

Reference:

<https://aws.amazon.com/products/databases/real-time-apps-elasticache-for-redis/>

QUESTION: 110

Which of the following is a component of the shared responsibility model managed entirely by AWS?

- A. Patching operating system software
- B. Encrypting data
- C. Enforcing multi-factor authentication
- D. Auditing physical data center assets

Answer(s): D**Explanation:**

Of course, Amazon is responsible for auditing physical data center assets and resources since it is the property of Amazon Inc. Customers have no access to physical sites, hence they are not responsible for maintaining physical data center assets.

QUESTION: 111

Which options does AWS make available for customers who want to learn about security in the cloud in an instructor-led setting? (Choose two.)

- A. AWS Trusted Advisor
- B. AWS Online Tech Talks
- C. AWS Blog
- D. AWS Forums
- E. AWS Classroom Training

Answer(s): B, E**QUESTION: 112**

Which of the following features can be configured through the Amazon Virtual Private Cloud (Amazon VPC) Dashboard? (Choose two.)

- A. Amazon CloudFront distributions

- B. Amazon Route 53
- C. Security Groups
- D. Subnets
- E. Elastic Load Balancing

Answer(s): C, D

Explanation:

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Reference:

<https://aws.amazon.com/vpc/>

QUESTION: 113

If each department within a company has its own AWS account, what is one way to enable consolidated billing?

- A. Use AWS Budgets on each account to pay only to budget
- B. Contact AWS Support for a monthly bill.
- C. Create an AWS Organization from the payer account and invite the other accounts to join.
- D. Put all invoices into one Amazon Simple Storage Service (Amazon S3) bucket, load data into Amazon Redshift, and then run a billing report.

Answer(s): C

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION: 114

How do customers benefit from Amazon's massive economies of scale?

- A. Periodic price reductions as the result of Amazon's operational efficiencies
- B. New Amazon EC2 instance types providing the latest hardware
- C. The ability to scale up and down when needed
- D. Increased reliability in the underlying hardware of Amazon EC2 instances

Answer(s): A

QUESTION: 115

Which AWS services can be used to gather information about AWS account activity? (Choose two.)

- A. Amazon CloudFront
- B. AWS Cloud9
- C. AWS CloudTrail
- D. AWS CloudHSM
- E. Amazon CloudWatch

Answer(s): C, E

Explanation:

AWS offers a solution that uses AWS CloudTrail to log account activity, Amazon Kinesis to compute and stream metrics in real-time, and Amazon DynamoDB to durably store the computed data. Metrics are calculated for create, modify, and delete API calls for more than 60 supported AWS services. The solution also features a dashboard that visualizes your account activity in real-time.

Reference:

<https://aws.amazon.com/solutions/real-time-insights-account-activity/>

QUESTION: 116

Which of the following common IT tasks can AWS cover to free up company IT resources? (Choose two.)

- A. Patching databases software
- B. Testing application releases
- C. Backing up databases
- D. Creating database schema
- E. Running penetration tests

Answer(s): A, C

QUESTION: 117

In which scenario should Amazon EC2 Spot Instances be used?

- A. A company wants to move its main website to AWS from an on-premises web server.
- B. A company has a number of application services whose Service Level Agreement (SLA) requires 99.999% uptime.
- C. A company's heavily used legacy database is currently running on-premises.
- D. A company has a number of infrequent, interruptible jobs that are currently using On-Demand Instances.

Answer(s): D

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-leveraging-ec2-spot-instances/spot-instance-interruptions.html>

QUESTION: 118

Which AWS feature should a customer leverage to achieve high availability of an application?

- A. AWS Direct Connect
- B. Availability Zones
- C. Data centers
- D. Amazon Virtual Private Cloud (Amazon VPC)

Answer(s): B

Explanation:

This is to achieve High Availability for any web application (in this case SwiftCode) deployed in AWS. The following features will be present:

- High availability across multiple instances/multiple availability zones.
- Auto Scaling of instances (scale up and scale down) based on number of requests coming in
- Additional Security to the instances/database that are in production
- No impact to end users during newer version of code deployment
- No Impact during patching the instances

Reference:

<https://betsol.com/2018/01/how-to-make-high-availability-web-applications-on-amazon-web-services/>

QUESTION: 119

Which is the minimum AWS Support plan that includes Infrastructure Event Management without additional costs?

- A. Enterprise
- B. Business
- C. Developer
- D. Basic

Answer(s): A

QUESTION: 120

Which AWS service can serve a static website?

- A. Amazon S3
- B. Amazon Route 53
- C. Amazon QuickSight
- D. AWS X-Ray

Answer(s): A

Explanation:

You can host a static website on Amazon Simple Storage Service (Amazon S3). On a static website, individual webpages include static content. They might also contain client-side scripts. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

QUESTION: 121

How does AWS shorten the time to provision IT resources?

- A. It supplies an online IT ticketing platform for resource requests.
- B. It supports automatic code validation services.
- C. It provides the ability to programmatically provision existing resources.
- D. It automates the resource request process from a company's IT vendor list.

Answer(s): C

QUESTION: 122

What can AWS edge locations be used for? (Choose two.)

- A. Hosting applications
- B. Delivering content closer to users
- C. Running NoSQL database caching services
- D. Reducing traffic on the server by caching responses
- E. Sending notification messages to end users

Answer(s): B, D

Explanation:

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

QUESTION: 123

Which of the following can limit Amazon Simple Storage Service (Amazon S3) bucket access to specific users?

- A. A public and private key-pair
- B. Amazon Inspector
- C. AWS Identity and Access Management (IAM) policies
- D. Security Groups

Answer(s): C

Explanation:

To allow users to perform S3 actions on the bucket from the VPC endpoints or IP addresses, you must explicitly grant those user-level permissions. You can grant user-level permissions on either an AWS Identity and Access Management (IAM) policy or another statement in the bucket policy.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/block-s3-traffic-vpc-ip/>

QUESTION: 124

A solution that is able to support growth in users, traffic, or data size with no drop in performance aligns with which cloud architecture principle?

- A. Think parallel
- B. Implement elasticity
- C. Decouple your components
- D. Design for failure

Answer(s): B

Reference:

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

QUESTION: 125

A company will be moving from an on-premises data center to the AWS Cloud. What would be one financial difference after the move?

- A. Moving from variable operational expense (opex) to upfront capital expense (capex).
- B. Moving from upfront capital expense (capex) to variable capital expense (capex).
- C. Moving from upfront capital expense (capex) to variable operational expense (opex).
- D. Elimination of upfront capital expense (capex) and elimination of variable operational expense (opex)

Answer(s): C

QUESTION: 126

How should a customer forecast the future costs for running a new web application?

- A. Amazon Aurora Backtrack
- B. Amazon CloudWatch Billing Alarms
- C. AWS Simple Monthly Calculator
- D. AWS Cost and Usage report

Answer(s): C

Explanation:

You can use Cost explorer which is part of Cost and Usage report to forecast future costs of running an application.

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-forecast.html>

QUESTION: 127

Which is the MINIMUM AWS Support plan that provides technical support through phone calls?

- A. Enterprise
- B. Business
- C. Developer
- D. Basic

Answer(s): B

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

QUESTION: 128

Which of the following tasks is the responsibility of AWS?

- A. Encrypting client-side data
- B. Configuring AWS Identity and Access Management (IAM) roles
- C. Securing the Amazon EC2 hypervisor
- D. Setting user password policies

Answer(s): C

Explanation:

In EC2, the AWS IaaS offering, everything from the hypervisor layer down is AWS's responsibility. A customer's poorly coded applications, misconfigured operating systems, or insecure firewall settings will not affect the hypervisor, it will only affect the customer's virtual machines running on that hypervisor.

Reference:

<https://www.mindpointgroup.com/blog/the-aws-shared-responsibility-model-part-1-security-in-the-cloud/>

QUESTION: 129

One benefit of On-Demand Amazon Elastic Compute Cloud (Amazon EC2) pricing is:

- A. the ability to bid for a lower hourly cost.
- B. paying a daily rate regardless of time used.
- C. paying only for time used.
- D. pre-paying for instances and paying a lower hourly rate.

Answer(s): C**Explanation:**

On-Demand Capacity Reservations are priced exactly the same as their equivalent (On-Demand) instance usage. If a Capacity Reservation is fully utilized, you only pay for instance usage and nothing towards the Capacity Reservation. If a Capacity Reservation is partially utilized, you pay for the instance usage and for the unused portion of the Capacity Reservation.

Reference:

<https://aws.amazon.com/ec2/pricing/on-demand/>

QUESTION: 130

An administrator needs to rapidly deploy a popular IT solution and start using it immediately. Where can the administrator find assistance?

- A. AWS Well-Architected Framework documentation
- B. Amazon CloudFront
- C. AWS CodeCommit
- D. AWS Quick Start reference deployments

Answer(s): D**Explanation:**

Quick Starts are built by AWS solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

Reference:

<https://aws.amazon.com/quickstart/?quickstart-all.sort-by=item.additionalFields.updateDate&quickstart-all.sort-order=desc>

QUESTION: 131

Which of the following services is in the category of AWS serverless platform?

- A. Amazon EMR

- B. Elastic Load Balancing
- C. AWS Lambda
- D. AWS Mobile Hub

Answer(s): C

Explanation:

AWS provides a set of fully managed services that you can use to build and run serverless applications. Serverless applications don't require provisioning, maintaining, and administering servers for backend components such as compute, databases, storage, stream processing, message queueing, and more. You also no longer need to worry about ensuring application fault tolerance and availability. Instead, AWS handles all of these capabilities for you. Serverless platform includes: AWS lambda, Amazon S3, DynamoDB, API gateway, Amazon SNS, AWS step functions, Amazon kinesis and developing tools and services.

Reference:

<https://aws.amazon.com/serverless/>

QUESTION: 132

Which services are parts of the AWS serverless platform?

- A. Amazon EC2, Amazon S3, Amazon Athena
- B. Amazon Kinesis, Amazon SQS, Amazon EMR
- C. AWS Step Functions, Amazon DynamoDB, Amazon SNS
- D. Amazon Athena, Amazon Cognito, Amazon EC2

Answer(s): C

Explanation:

AWS provides a set of fully managed services that you can use to build and run serverless applications. Serverless applications don't require provisioning, maintaining, and administering servers for backend components such as compute, databases, storage, stream processing, message queueing, and more. You also no longer need to worry about ensuring application fault tolerance and availability. Instead, AWS handles all of these capabilities for you. Serverless platform includes: AWS lambda, Amazon S3, DynamoDB, API gateway, Amazon SNS, AWS step functions, Amazon kinesis and developing tools and services.

Reference:

<https://aws.amazon.com/serverless/>

QUESTION: 133

According to the AWS shared responsibility model, what is the sole responsibility of AWS?

- A. Application security
- B. Edge location management
- C. Patch management

D. Client-side data

Answer(s): B

Explanation:

Client-side data, application security is the sole responsibility of the customer. Patch management is a shared responsibility. That leaves us with edge location management and since this is out of the control of the customer, AWS is the one responsible for it.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 134

Which AWS IAM feature is used to associate a set of permissions with multiple users?

- A. Multi-factor authentication
- B. Groups
- C. Password policies
- D. Access keys

Answer(s): B

Explanation:

An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users. For example, you could have a group called Admins and give that group the types of permissions that administrators typically need.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html>

QUESTION: 135

Which of the following are benefits of the AWS Cloud? (Choose two.)

- A. Unlimited uptime
- B. Elasticity
- C. Agility
- D. Colocation
- E. Capital expenses

Answer(s): B, C

Explanation:

The most celebrated benefit of AWS cloud is elasticity since you can expand the services when you experience more traffic.

Agile developments in AWS Cloud through strategies are day by day becoming more established within the enterprises across the world. With so much improvement and call for optimization in the cloud, it is necessary that these strategies get established from the ground

up within the organizations. It is highly important as already enterprises have a lot of bequest, politics and hierarchies which act as barriers in their businesses.

Reference:

<https://www.botmetric.com/blog/evolution-agile-enterprises-aws-cloud/>

QUESTION: 136

Which of the following can a customer use to enable single sign-on (SSO) to the AWS Console?

- A. Amazon Connect
- B. AWS Directory Service
- C. Amazon Pinpoint
- D. Amazon Rekognition

Answer(s): B**Explanation:**

Single sign-on only works when used on a computer that is joined to the AWS Directory Service directory. It cannot be used on computers that are not joined to the directory.

Reference:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_single_sign_on.html

QUESTION: 137

What are the multiple, isolated locations within an AWS Region that are connected by low-latency networks called?

- A. AWS Direct Connects
- B. Amazon VPCs
- C. Edge locations
- D. Availability Zones

Answer(s): D**Explanation:**

Each Region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a Region are connected through low-latency links. A Local Zone is an AWS infrastructure deployment that places select services closer to your end users. A Local Zone is an extension of a Region that is in a different location from your Region. It provides a high-bandwidth backbone to the AWS infrastructure and is ideal for latency-sensitive applications, for example machine learning.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

QUESTION: 138

Which of the following benefits does the AWS Compliance program provide to AWS customers? (Choose two.)

- A. It verifies that hosted workloads are automatically compliant with the controls of supported compliance frameworks.
- B. AWS is responsible for the maintenance of common compliance framework documentation.
- C. It assures customers that AWS is maintaining physical security and data protection.
- D. It ensures the use of compliance frameworks that are being used by other cloud providers.
- E. It will adopt new compliance frameworks as they become relevant to customer workloads.

Answer(s): B, C

Reference:

https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

QUESTION: 139

Which of the following services provides on-demand access to AWS compliance reports?

- A. AWS IAM
- B. AWS Artifact
- C. Amazon GuardDuty
- D. AWS KMS

Answer(s): B

Explanation:

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Reference:

<https://aws.amazon.com/artifact/>

QUESTION: 140

As part of the AWS shared responsibility model, which of the following operational controls do users fully inherit from AWS?

- A. Security management of data center
- B. Patch management
- C. Configuration management
- D. User and access management

Answer(s): A

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 141

When comparing AWS Cloud with on-premises Total Cost of Ownership, which expenses must be considered? (Choose two.)

- A. Software development
- B. Project management
- C. Storage hardware
- D. Physical servers
- E. Antivirus software license

Answer(s): C, D

Reference:

<https://aws.amazon.com/blogs/aws/the-new-aws-tco-calculator/>

QUESTION: 142

Under the shared responsibility model, which of the following tasks are the responsibility of the customer? (Choose two.)

- A. Maintaining the underlying Amazon EC2 hardware.
- B. Managing the VPC network access control lists.
- C. Encrypting data in transit and at rest.
- D. Replacing failed hard disk drives.
- E. Deploying hardware in different Availability Zones.

Answer(s): B, C

Explanation:

The hardware related jobs is the prime responsibility of AWS. VPC network access control lists is something a customer has to do himself to secure the applications. Encrypting data in transit and at rest is a shared responsibility in which AWS plays a part. All hardware related jobs have nothing to do with the customer.

Reference:

<https://dzone.com/articles/aws-shared-responsibility-model-cloud-security>

QUESTION: 143

Which scenarios represent the concept of elasticity on AWS? (Choose two.)

- A. Scaling the number of Amazon EC2 instances based on traffic.
- B. Resizing Amazon RDS instances as business needs change.
- C. Automatically directing traffic to less-utilized Amazon EC2 instances.
- D. Using AWS compliance documents to accelerate the compliance process.

E. Having the ability to create and govern environments using code.

Answer(s): A, B

Reference:

<https://wa.aws.amazon.com/wat.concept.elasticity.en.html>

QUESTION: 144

When is it beneficial for a company to use a Spot Instance?

- A. When there is flexibility in when an application needs to run.
- B. When there are mission-critical workloads.
- C. When dedicated capacity is needed.
- D. When an instance should not be stopped.

Answer(s): A

Explanation:

The key to understanding spot instances is to look at the way that cloud service providers such as Amazon Web Services (AWS) operate. Cloud service providers invest in hardware resources and then release those resources (often on a per-hour basis) to subscribers. One of the problems with this business model, however, is that at any given time, there are likely to be compute resources that are not being utilized. These resources represent hardware capacity that AWS has paid for but are sitting idle, and not making AWS any money at the moment.

Rather than allowing these computing resources to go to waste, AWS offers them at a substantially discounted rate, with the understanding that if someone needs those resources for running a normal EC2 instance, that instance will take priority over spot instances that are using the hardware resources at a discounted rate. In fact, spot instances will be stopped if the resources are needed elsewhere.

Reference:

<https://awsinsider.net/articles/2017/09/25/aws-spot-instances-primer.aspx>

QUESTION: 145

A company is considering moving its on-premises data center to AWS.

What factors should be included in doing a Total Cost of Ownership (TCO) analysis? (Choose two.)

- A. Amazon EC2 instance availability
- B. Power consumption of the data center
- C. Labor costs to replace old servers
- D. Application developer time
- E. Database engine capacity

Answer(s): B, C

QUESTION: 146

How does AWS charge for AWS Lambda?

- A. Users bid on the maximum price they are willing to pay per hour.
- B. Users choose a 1-, 3- or 5-year upfront payment term.
- C. Users pay for the required permanent storage on a file system or in a database.
- D. Users pay based on the number of requests and consumed compute resources.

Answer(s): D

Explanation:

AWS Lambda is charging its users by the number of requests for their functions and by the duration, which is the time the code needs to execute. When code starts running in response to an event, AWS Lambda counts a request. It will charge the total number of requests across all of the functions used. Duration is calculated by the time when your code started executing until it returns or until it is terminated, rounded up near to 100ms.

The AWS Lambda pricing depends on the amount of memory that the user used to allocate to the function.

Reference:

<https://dashbird.io/blog/aws-lambda-pricing-model-explained/>

QUESTION: 147

What function do security groups serve related Amazon Elastic Compute Cloud (Amazon EC2) instance security?

- A. Act as a virtual firewall for the Amazon EC2 instance.
- B. Secure AWS user accounts with AWS Identity and Access Management (IAM) policies.
- C. Provide DDoS protection with AWS Shield
- D. Use Amazon CloudFront to protect the Amazon EC2 instance.

Answer(s): A

Explanation:

AWS Security Groups act like a firewall for your Amazon EC2 instances controlling both inbound and outbound traffic. When you launch an instance on Amazon EC2, you need to assign it to a particular security group.

After that, you can set up ports and protocols, which remain open for users and computers over the internet.

AWS Security Groups are very flexible. You can use the default security group and still customize it according to your liking (although we don't recommend this practice because groups should be named according to their purpose.) Or you can create a security group that you want for your specific applications. To do this, you can write the corresponding code or use the Amazon EC2 console to make the process easier.

Reference:

<https://www.threatstack.com/blog/aws-security-groups-what-they-are-and-how-to-get-the-most-out-of-them>

QUESTION: 148

Which disaster recovery scenario offers the lowest probability of down time?

- A. Backup and restore
- B. Pilot light
- C. Warm standby
- D. Multi-site active-active

Answer(s): D**Explanation:**

- Backup and Restore: a simple, straightforward, cost-effective method that backs up and restores data as needed. Keep in mind that because none of your data is on standby, this method, while cheap, can be quite time-consuming.
- Pilot Light: This method keeps critical applications and data at the ready so that it can be quickly retrieved if needed.
- Warm Standby: This method keeps a duplicate version of your business' core elements running on standby at all times, which makes for a little downtime and an almost seamless transition.
- Multi-Site Solution: Also known as a Hot Standby, this method fully replicates your company's data/ applications between two or more active locations and splits your traffic/usage between them. If a disaster strikes, everything is simply rerouted to the unaffected area, which means you'll suffer almost zero downtime. However, by running two separate environments simultaneously, you will obviously incur much higher costs.

Reference:

<https://cloudranger.com/best-practices-aws-disaster-recovery-planning/>

QUESTION: 149

What will help a company perform a cost benefit analysis of migrating to the AWS Cloud?

- A. Cost Explorer
- B. AWS Total Cost of Ownership (TCO) Calculator
- C. AWS Simple Monthly Calculator
- D. AWS Trusted Advisor

Answer(s): B**Explanation:**

AWS TCO calculators allow you to estimate the cost savings when using AWS and provide a detailed set of reports that can be used in executive presentations. The calculators also give

you the option to modify assumptions that best meet your business needs.

Reference:

<https://aws.amazon.com/tco-calculator/>

QUESTION: 150

Which of the following provides the ability to share the cost benefits of Reserved Instances across AWS accounts?

- A. AWS Cost Explorer between AWS accounts
- B. Linked accounts and consolidated billing
- C. Amazon Elastic Compute Cloud (Amazon EC2) Reserved Instance Utilization Report
- D. Amazon EC2 Instance Usage Report between AWS accounts

Answer(s): B

Explanation:

The way that Reserved Instance discounts apply to accounts in an organization's consolidated billing family depends on whether Reserved Instance sharing is turned on or off for the account. By default, Reserved Instance sharing for all accounts in an organization is turned on. You can change this setting by Turning Off Reserved Instance Sharing for an account.

The capacity reservation for a Reserved Instance applies only to the account the Reserved Instance was purchased on, regardless of whether Reserved Instance sharing is turned on or off.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/>

QUESTION: 151

A company has multiple AWS accounts and wants to simplify and consolidate its billing process. Which AWS service will achieve this?

- A. AWS Cost and Usage Reports
- B. AWS Organizations
- C. AWS Cost Explorer
- D. AWS Budgets

Answer(s): B

Explanation:

You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. Every organization in AWS Organizations has a master (payer) account that pays the charges of all the member (linked) accounts.

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION: 152

A company is designing an application hosted in a single AWS Region serving end-users spread across the world. The company wants to provide the end-users low latency access to the application data.

Which of the following services will help fulfill this requirement?

- A. Amazon CloudFront
- B. AWS Direct Connect
- C. Amazon Route 53 global DNS
- D. Amazon Simple Storage Service (Amazon S3) transfer acceleration

Answer(s): A

Explanation:

Use AWS Local Zones to deploy workloads closer to your end-users for low-latency requirements. AWS Local Zones have their own connection to the internet and support AWS Direct Connect, so resources created in the Local Zone can serve local end-users with very low-latency communications.

Reference:

<https://aws.amazon.com/about-aws/global-infrastructure/localzones/faqs/>

QUESTION: 153

Which of the following deployment models enables customers to fully trade their capital IT expenses for operational expenses?

- A. On-premises
- B. Hybrid
- C. Cloud
- D. Platform as a service

Answer(s): C

Explanation:

The cloud allows you to trade capital expenses (such as data centers and physical servers) for variable expenses, and only pay for IT as you consume it. Plus, the variable expenses are much lower than what you would pay to do it yourself because of the economies of scale.

Reference:

<https://aws.amazon.com/what-is-cloud-computing/>

QUESTION: 154

How is asset management on AWS easier than asset management in a physical data center?

- A. AWS provides a Configuration Management Database that users can maintain.
- B. AWS performs infrastructure discovery scans on the customer's behalf.

- C. Amazon EC2 automatically generates an asset report and places it in the customer's specified Amazon S3 bucket.
- D. Users can gather asset metadata reliably with a few API calls.

Answer(s): B

Explanation:

AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

Reference:

<https://aws.amazon.com/compliance/data-center/controls/>

QUESTION: 155

What feature of Amazon RDS helps to create globally redundant databases?

- A. Snapshots
- B. Automatic patching and updating
- C. Cross-Region read replicas
- D. Provisioned IOPS

Answer(s): C

Reference:

<https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/>

QUESTION: 156

Using AWS Identity and Access Management (IAM) to grant access only to the resources needed to perform a task is a concept known as:

- A. restricted access.
- B. as-needed access.
- C. least privilege access.
- D. token access.

Answer(s): C

Explanation:

When you create IAM policies, follow the standard security advice of granting least privilege, or granting only the permissions required to perform a task. Determine what users (and roles) need to do and then craft policies that allow them to perform only those tasks.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

QUESTION: 157

Which methods can be used to identify AWS costs by departments? (Choose two.)

- A. Enable multi-factor authentication for the AWS account root user.
- B. Create separate accounts for each department.
- C. Use Reserved Instances whenever possible.
- D. Use tags to associate each instance with a particular department.
- E. Pay bills using purchase orders.

Answer(s): B, D

QUESTION: 158

Under the AWS shared responsibility model, customer responsibilities include which one of the following?

- A. Securing the hardware, software, facilities, and networks that run all products and services.
- B. Providing certificates, reports, and other documentation directly to AWS customers under NDA.
- C. Configuring the operating system, network, and firewall.
- D. Obtaining industry certifications and independent third-party attestations.

Answer(s): C

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 159

Which managed AWS service provides real-time guidance on AWS security best practices?

- A. AWS X-Ray
- B. AWS Trusted Advisor
- C. Amazon CloudWatch
- D. AWS Systems Manager

Answer(s): B

Explanation:

AWS offers premium services such as AWS Trusted Advisor, which provides real-time guidance to help you reduce cost, increase performance, and improve security.

Reference:

<https://www.ibm.com/downloads/cas/2N40X4PQ>

QUESTION: 160

Which feature adds elasticity to Amazon EC2 instances to handle the changing demand for workloads?

- A. Resource groups
- B. Lifecycle policies

- C. Application Load Balancer
- D. Amazon EC2 Auto Scaling

Answer(s): D

Explanation:

Support for monitoring the health of each service independently, as health checks are defined at the target group level and many CloudWatch metrics are reported at the target group level. Attaching a target group to an Auto Scaling group enables you to scale each service dynamically based on demand.

Reference:

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

QUESTION: 161

Under the AWS shared responsibility model, customers are responsible for which aspects of security in the cloud? (Choose two.)

- A. Visualization management
- B. Hardware management
- C. Encryption management
- D. Facilities management
- E. Firewall management

Answer(s): C, E

Explanation:

With the basic Cloud infrastructure secured and maintained by AWS, the responsibility for what goes into the cloud falls on you. This covers both client and server side encryption and network traffic protection, security of the operating system, network, and firewall configuration, followed by application security and identity and access management.

Firewall configuration remains the responsibility of the end user, which integrates at the platform and application management level. For example, RDS utilizes security groups, which you would be responsible for configuring and implementing.

Reference:

<https://cloudacademy.com/blog/aws-shared-responsibility-model-security/>

QUESTION: 162

Which AWS hybrid storage service enables on-premises applications to seamlessly use AWS Cloud storage through standard file-storage protocols?

- A. AWS Direct Connect
- B. AWS Snowball
- C. AWS Storage Gateway
- D. AWS Snowball Edge

Answer(s): C

Explanation:

The AWS Storage Gateway service enables hybrid cloud storage between on-premises environments and the AWS Cloud. It seamlessly integrates on-premises enterprise applications and workflows with Amazon's block and object cloud storage services through industry standard storage protocols. It provides low-latency performance by caching frequently accessed data on premises, while storing data securely and durably in Amazon cloud storage services. It provides an optimized data transfer mechanism and bandwidth management, which tolerates unreliable networks and minimizes the amount of data being transferred. It brings the security, manageability, durability, and scalability of AWS to existing enterprise environments through native integration with AWS encryption, identity management, monitoring, and storage services. Typical use cases include backup and archiving, disaster recovery, moving data to S3 for in-cloud workloads, and tiered storage.

Reference:

<https://aws.amazon.com/storagegateway/faqs/>

QUESTION: 163

What is a responsibility of AWS in the shared responsibility model?

- A. Updating the network ACLs to block traffic to vulnerable ports.
- B. Patching operating systems running on Amazon EC2 instances.
- C. Updating the firmware on the underlying EC2 hosts.
- D. Updating the security group rules to block traffic to the vulnerable ports.

Answer(s): C**Reference:**

<https://cloudacademy.com/blog/aws-shared-responsibility-model-security/>

QUESTION: 164

Which architectural principle is used when deploying an Amazon Relational Database Service (Amazon RDS) instance in Multiple Availability Zone mode?

- A. Implement loose coupling.
- B. Design for failure.
- C. Automate everything that can be automated.
- D. Use services, not servers.

Answer(s): B**Explanation:**

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover

to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

Reference:

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

QUESTION: 165

What does it mean to grant least privilege to AWS IAM users?

- A. It is granting permissions to a single user only.
- B. It is granting permissions using AWS IAM policies only.
- C. It is granting AdministratorAccess policy permissions to trustworthy users.
- D. It is granting only the permissions required to perform a given task.

Answer(s): D**Explanation:**

When you create IAM policies, follow the standard security advice of granting least privilege, or granting only the permissions required to perform a task. Determine what users (and roles) need to do and then craft policies that allow them to perform only those tasks.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege>

QUESTION: 166

What is a benefit of loose coupling as a principle of cloud architecture design?

- A. It facilitates low-latency request handling.
- B. It allows applications to have dependent workflows.
- C. It prevents cascading failures between different components.
- D. It allows companies to focus on their physical data center operations.

Answer(s): C**Explanation:**

IT systems should ideally be designed in a way that reduces inter-dependencies. Your components need to be loosely coupled to avoid changes or failure in one of the components from affecting others.

Your infrastructure also needs to have well defined interfaces that allow the various components to interact with each other only through specific, technology-agnostic interfaces. Modifying any underlying operations without affecting other components should be made possible.

Reference:

<https://www.botmetric.com/blog/aws-cloud-architecture-design-principles/>

QUESTION: 167

A director has been tasked with investigating hybrid cloud architecture. The company currently accesses AWS over the public internet.

Which service will facilitate private hybrid connectivity?

- A. Amazon Virtual Private Cloud (Amazon VPC) NAT Gateway
- B. AWS Direct Connect
- C. Amazon Simple Storage Service (Amazon S3) Transfer Acceleration
- D. AWS Web Application Firewall (AWS WAF)

Answer(s): B

Explanation:

Amazon VPC provides multiple network connectivity options for you to leverage depending on your current network designs and requirements. These connectivity options include leveraging either the internet or an AWS Direct Connect connection as the network backbone and terminating the connection into either AWS or user-managed network endpoints. Additionally, with AWS, you can choose how network routing is delivered between Amazon VPC and your networks, leveraging either AWS or user-managed network equipment and routes.

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/introduction.html>

QUESTION: 168

A company's web application currently has tight dependencies on underlying components, so when one component fails the entire web application fails. Applying which AWS Cloud design principle will address the current design issue?

- A. Implementing elasticity, enabling the application to scale up or scale down as demand changes.
- B. Enabling several EC2 instances to run in parallel to achieve better performance.
- C. Focusing on decoupling components by isolating them and ensuring individual components can function when other components fail.
- D. Doubling EC2 computing resources to increase system fault tolerance.

Answer(s): C

QUESTION: 169

How can a customer increase security to AWS account logons? (Choose two.)

- A. Configure AWS Certificate Manager
- B. Enable Multi-Factor Authentication (MFA)
- C. Use Amazon Cognito to manage access
- D. Configure a strong password policy
- E. Enable AWS Organizations

Answer(s): B, C

Explanation:

Your root account should always be protected by Multi-Factor Authentication (MFA). This additional layer of security helps protect against unauthorized logins to your account by requiring two factors: something you know (a password) and something you have (for example, an MFA device). AWS supports virtual and hardware MFA devices and U2F security keys.

Cognito can be used as an Identity Provider (IdP), where it stores and maintains users and credentials securely for your applications, or it can be integrated with OpenID Connect, SAML, and other popular web identity providers like Amazon.com.

Using Amazon Cognito, you can generate temporary access credentials for your clients to access AWS services, eliminating the need to store long-term credentials in client applications.

Reference:

<https://aws.amazon.com/blogs/security/guidelines-for-protecting-your-aws-account-while-using-programmatic-access/>

QUESTION: 170

What AWS service would be used to centrally manage AWS access across multiple accounts?

- A. AWS Service Catalog
- B. AWS Config
- C. AWS Trusted Advisor
- D. AWS Organizations

Answer(s): D

Explanation:

To improve control over your AWS environment, you can use AWS Organizations to create groups of accounts, and then attach policies to a group to ensure the correct policies are applied across the accounts without requiring custom scripts and manual processes.

Reference:

<https://aws.amazon.com/organizations/>

QUESTION: 171

Which AWS service can a customer use to set up an alert notification when the account is approaching a particular dollar amount?

- A. AWS Cost and Usage reports
- B. AWS Budgets
- C. AWS Cost Explorer
- D. AWS Trusted Advisor

Answer(s): B

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charge_s_with_cloudwatch.html

QUESTION: 172

What can users access from AWS Artifact?

- A. AWS security and compliance documents
- B. A download of configuration management details for all AWS resources
- C. Training materials for AWS services
- D. A security assessment of the applications deployed in the AWS Cloud

Answer(s): A

Explanation:

You can use AWS Artifact Reports to download AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and System and Organization Control (SOC) reports.

Reference:

<https://aws.amazon.com/artifact/faq/>

QUESTION: 173

Which is the MINIMUM AWS Support plan that provides designated Technical Account Managers?

- A. Enterprise
- B. Business
- C. Developer
- D. Basic

Answer(s): A

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

QUESTION: 174

Which of the following is an AWS Well-Architected Framework design principle related to reliability?

- A. Deployment to a single Availability Zone
- B. Ability to recover from failure
- C. Design for cost optimization
- D. Perform operations as code

Answer(s): B

Reference:

<https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/>

QUESTION: 175

Which type of AWS storage is ephemeral and is deleted when an instance is stopped or terminated?

- A. Amazon EBS
- B. Amazon EC2 instance store
- C. Amazon EFS
- D. Amazon S3

Answer(s): B**Explanation:**

When you stop or terminate an instance, every block of storage in the instance store is reset. Therefore, your data cannot be accessed through the instance store of another instance.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

QUESTION: 176

What is an advantage of using the AWS Cloud over a traditional on-premises solution?

- A. Users do not have to guess about future capacity needs.
- B. Users can utilize existing hardware contracts for purchases.
- C. Users can fix costs no matter what their traffic is.
- D. Users can avoid audits by using reports from AWS.

Answer(s): A**Reference:**

<https://data-flair.training/blogs/aws-advantages/>

QUESTION: 177

Which of the following is an AWS-managed compute service?

- A. Amazon SWF
- B. Amazon EC2
- C. AWS Lambda
- D. Amazon Aurora

Answer(s): B**QUESTION: 178**

Which of the following is an important architectural principle when designing cloud applications?

- A. Store data and backups in the same region.
- B. Design tightly coupled system components.
- C. Avoid multi-threading.
- D. Design for failure

Answer(s): D

Explanation:

There are six design principles for operational excellence in the cloud:

- Perform operations as code
- Annotate documentation
- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures

Reference:

<https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/>

QUESTION: 179

Which mechanism allows developers to access AWS services from application code?

- A. AWS Software Development Kit
- B. AWS Management Console
- C. AWS CodePipeline
- D. AWS Config

Answer(s): A

Reference:

<https://aws.amazon.com/tools/>

QUESTION: 180

Which Amazon EC2 pricing model is the MOST cost efficient for an uninterruptible workload that runs once a year for 24 hours?

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

Answer(s): A

Explanation:

With On-Demand instances, you pay for compute capacity by the hour or the second depending on which instances you run. No longer-term commitments or upfront payments are needed. You

can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.

Reference:

<https://aws.amazon.com/ec2/pricing/>

QUESTION: 181

Which of the following services is a MySQL-compatible database that automatically grows storage as needed?

- A. Amazon Elastic Compute Cloud (Amazon EC2)
- B. Amazon Relational Database Service (Amazon RDS) for MySQL
- C. Amazon Lightsail
- D. Amazon Aurora

Answer(s): D

Explanation:

Amazon Aurora is a relational database service that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases. The MySQL- compatible edition of Aurora delivers up to 5X the throughput of standard MySQL running on the same hardware, and enables existing MySQL applications and tools to run without requiring modification.

Amazon Aurora will automatically grow the size of your database volume as your database storage needs grow. Your volume will grow in increments of 10 GB up to a maximum of 64 TB. You don't need to provision excess storage for your database to handle future growth.

Reference:

<https://aws.amazon.com/rds/aurora/mysql-features/>

QUESTION: 182

Which Amazon Virtual Private Cloud (Amazon VPC) feature enables users to connect two VPCs together?

- A. Amazon VPC endpoints
- B. Amazon Elastic Compute Cloud (Amazon EC2) ClassicLink
- C. Amazon VPC peering
- D. AWS Direct Connect

Answer(s): C

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

Reference:

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

QUESTION: 183

Which service's PRIMARY purpose is software version control?

- A. Amazon CodeStar
- B. AWS Command Line Interface (AWS CLI)
- C. Amazon Cognito
- D. AWS CodeCommit

Answer(s): D**Explanation:**

AWS CodeCommit is a version control service hosted by Amazon Web Services that you can use to privately store and manage assets (such as documents, source code, and binary files) in the cloud.

Reference:

<https://docs.aws.amazon.com/codecommit/latest/userguide/welcome.html>

QUESTION: 184

A company is considering migrating its applications to AWS. The company wants to compare the cost of running the workload on-premises to running the equivalent workload on the AWS platform.

Which tool can be used to perform this comparison?

- A. AWS Simple Monthly Calculator
- B. AWS Total Cost of Ownership (TCO) Calculator
- C. AWS Billing and Cost Management console
- D. Cost Explorer

Answer(s): B**Explanation:**

TCO calculator compare the cost of running your applications in an on-premises or colocation environment to AWS.

Reference:

<https://awstcoccalculator.com>

QUESTION: 185

Which AWS service provides a secure, fast, and cost-effective way to migrate or transport exabyte-scale datasets into AWS?

- A. AWS Batch
- B. AWS Snowball
- C. AWS Migration Hub

D. AWS Snowmobile

Answer(s): D

Explanation:

AWS Snowmobile is an exabyte-scale data transfer service that can move extremely large amounts of data to AWS in a fast, secure, and cost-effective manner. You can transfer up to 100PB per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. All data is encrypted with 256-bit encryption and you can manage your encryption keys with AWS Key Management Service (AWS KMS). Snowmobile includes GPS tracking, alarm monitoring, 24/7 video surveillance and an optional escort security vehicle while in transit.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2016/11/move-exabyte-scale-data-sets-with-aws-snowmobile/>

QUESTION: 186

Which of the following BEST describe the AWS pricing model? (Choose two.)

- A. Fixed-term
- B. Pay-as-you-go
- C. Colocation
- D. Planned
- E. Variable cost

Answer(s): B, E

Reference:

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

QUESTION: 187

Which load balancer types are available with Elastic Load Balancing (ELB)? (Choose two.)

- A. Public load balancers with AWS Application Auto Scaling capabilities
- B. F5 Big-IP and Citrix NetScaler load balancers
- C. Classic Load Balancers
- D. Cross-zone load balancers with public and private IPs
- E. Application Load Balancers

Answer(s): C, E

Explanation:

Elastic Load Balancing supports the following types of load balancers: Application Load Balancers, Network Load Balancers, and Classic Load Balancers. Amazon ECS services can use either type of load balancer. Application Load Balancers are used to route HTTP/HTTPS (or

Layer 7) traffic. Network Load Balancers and Classic Load Balancers are used to route TCP (or Layer 4) traffic.

Reference:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/load-balancer-types.html>

QUESTION: 188

Why should a company choose AWS instead of a traditional data center?

- A. AWS provides users with full control over the underlying resources.
- B. AWS does not require long-term contracts and provides a pay-as-you-go model.
- C. AWS offers edge locations in every country, supporting global reach.
- D. AWS has no limits on the number of resources that can be created.

Answer(s): B

Explanation:

AWS offers you a pay-as-you-go approach for pricing for over 160 cloud services. With AWS you pay only for the individual services you need, for as long as you use them, and without requiring long-term contracts or complex licensing. AWS pricing is similar to how you pay for utilities like water and electricity. You only pay for the services you consume, and once you stop using them, there are no additional costs or termination fees.

Reference:

<https://aws.amazon.com/pricing/>

QUESTION: 189

Which solution provides the FASTEST application response times to frequently accessed data to users in multiple AWS Regions?

- A. AWS CloudTrail across multiple Availability Zones
- B. Amazon CloudFront to edge locations
- C. AWS CloudFormation in multiple regions
- D. A virtual private gateway over AWS Direct Connect

Answer(s): B

Explanation:

You can deliver content and decrease end-user latency of your web application using Amazon CloudFront. CloudFront speeds up content delivery by leveraging its global network of data centers, known as edge locations, to reduce delivery time by caching your content close to your end users. CloudFront fetches your content from an origin, such as an Amazon S3 bucket, an Amazon EC2 instance, an Amazon Elastic Load Balancing load balancer or your own web server, when it's not already in an edge location. CloudFront can be used to deliver your entire website or application, including dynamic, static, streaming, and interactive content.

Reference:

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

QUESTION: 190

Which AWS service provides a self-service portal for on-demand access to AWS compliance reports?

- A. AWS Config
- B. AWS Certificate Manager
- C. Amazon Inspector
- D. AWS Artifact

Answer(s): D**Explanation:**

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Reference:

<https://aws.amazon.com/artifact/>

QUESTION: 191

Which of the following AWS services can be used to run a self-managed database?

- A. Amazon Route 53
- B. AWS X-Ray
- C. AWS Snowmobile
- D. Amazon Elastic Compute Cloud (Amazon EC2)

Answer(s): D**Reference:**

<https://severalnines.com/news/aws-users-prefer-self-managed-databases>

QUESTION: 192

What exclusive benefit is provided to users with Enterprise Support?

- A. Access to a Technical Project Manager
- B. Access to a Technical Account Manager
- C. Access to a Cloud Support Engineer
- D. Access to a Solutions Architect

Answer(s): B**Reference:**

<https://aws.amazon.com/premiumsupport/plans/enterprise/>

QUESTION: 193

How can a user protect against AWS service disruptions if a natural disaster affects an entire geographic area?

- A. Deploy applications across multiple Availability Zones within an AWS Region.
- B. Use a hybrid cloud computing deployment model within the geographic area.
- C. Deploy applications across multiple AWS Regions.
- D. Store application artifacts using AWS Artifact and replicate them across multiple AWS Regions.

Answer(s): C**Explanation:**

An AWS Region is a geographic location where AWS provides multiple, physically separated and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking.

Reference:

<https://aws.amazon.com/s3/faqs/>

QUESTION: 194

How does AWS MOST effectively reduce computing costs for a growing start-up company?

- A. It provides on-demand resources for peak usage.
- B. It automates the provisioning of individual developer environments.
- C. It automates customer relationship management.
- D. It implements a fixed monthly computing budget.

Answer(s): A**Explanation:**

You can continue to optimize your spend and keep your development costs low by making sure you revisit your architecture often, to adjust to your startup growth. Manage your cost further by leveraging different options such as S3 CloudFront for caching & offloading to reduce cost of EC2 computing, as well as Elastic Load Balancing which prepares you for massive scale, high reliability and uninterrupted growth. Another way to keep costs down is to use AWS Identity and Access Management solutions (IAM) to manage governance of your cost drivers effectively and by the right teams.

Reference:

<https://aws.amazon.com/startups/lean/>

QUESTION: 195

A startup is working on a new application that needs to go to market quickly. The application requirements may need to be adjusted in the near future.

Which of the following is a characteristic of the AWS Cloud that would meet this specific need?

- A. Elasticity
- B. Reliability
- C. Performance
- D. Agility

Answer(s): D

Explanation:

Agile is a time boxed, iterative approach to software delivery that builds software incrementally from the start of the project, instead of trying to deliver it all at once near the end.

Reference:

<http://www.agilenutshell.com>

QUESTION: 196

Which AWS Support plan provides a full set of AWS Trusted Advisor checks?

- A. Business and Developer Support
- B. Business and Basic Support
- C. Enterprise and Developer Support
- D. Enterprise and Business Support

Answer(s): D

QUESTION: 197

Which of the following services have Distributed Denial of Service (DDoS) mitigation features? (Choose two.)

- A. AWS WAF
- B. Amazon DynamoDB
- C. Amazon EC2
- D. Amazon CloudFront
- E. Amazon Inspector

Answer(s): A, D

Reference:

<https://aws.amazon.com/shield/>

QUESTION: 198

When building a cloud Total Cost of Ownership (TCO) model, which cost elements should be considered for workloads running on AWS? (Choose three.)

- A. Compute costs
- B. Facilities costs

- C. Storage costs
- D. Data transfer costs
- E. Network infrastructure costs
- F. Hardware lifecycle costs

Answer(s): A, C, E

Reference:

<https://aws.amazon.com/blogs/aws/the-new-aws-tco-calculator/>

QUESTION: 199

What time-savings advantage is offered with the use of Amazon Rekognition?

- A. Amazon Rekognition provides automatic watermarking of images.
- B. Amazon Rekognition provides automatic detection of objects appearing in pictures.
- C. Amazon Rekognition provides the ability to resize millions of images automatically.
- D. Amazon Rekognition uses Amazon Mechanical Turk to allow humans to bid on object detection jobs.

Answer(s): B

Explanation:

Rekognition Image is an image recognition service that detects objects, scenes, and faces; extracts text; recognizes celebrities; and identifies inappropriate content in images. It also allows you to search and compare faces. Rekognition Image is based on the same proven, highly scalable, deep learning technology developed by Amazon's computer vision scientists to analyze billions of images daily for Prime Photos.

Reference:

<https://aws.amazon.com/rekognition/faqs/>

QUESTION: 200

When comparing AWS with on-premises Total Cost of Ownership (TCO), what costs are included?

- A. Data center security
- B. Business analysis
- C. Project management
- D. Operating system administration

Answer(s): A

Reference:

<https://www.awstcoccalculator.com/Output/Load/f85bbf7e131446643911859504>

QUESTION: 201

According to the AWS shared responsibility model, what is AWS responsible for?

- A. Configuring Amazon VPC
- B. Managing application code
- C. Maintaining application traffic
- D. Managing the network infrastructure

Answer(s): D

Reference:

<https://cloudacademy.com/blog/aws-shared-responsibility-model-security/>

QUESTION: 202

Which service should be used to estimate the costs of running a new project on AWS?

- A. AWS TCO Calculator
- B. AWS Simple Monthly Calculator
- C. AWS Cost Explorer API
- D. AWS Budgets

Answer(s): B

Explanation:

To forecast your costs, use the AWS Cost Explorer. Use cost allocation tags to divide your resources into groups, and then estimate the costs for each group.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/estimating-aws-resource-costs/>

QUESTION: 203

Which AWS tool will identify security groups that grant unrestricted Internet access to a limited list of ports?

- A. AWS Organizations
- B. AWS Trusted Advisor
- C. AWS Usage Report
- D. Amazon EC2 dashboard

Answer(s): B

QUESTION: 204

Which AWS service can be used to generate alerts based on an estimated monthly bill?

- A. AWS Config
- B. Amazon CloudWatch
- C. AWS X-Ray
- D. AWS CloudTrail

Answer(s): B

Explanation:

You can monitor your estimated AWS charges by using Amazon CloudWatch. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.

Billing metric data is stored in the US East (N. Virginia) Region and represents worldwide charges. This data includes the estimated charges for every service in AWS that you use, in addition to the estimated overall total of your AWS charges.

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charges_with_cloudwatch.html

QUESTION: 205

Which Amazon EC2 pricing model offers the MOST significant discount when compared to On-Demand Instances?

- A. Partial Upfront Reserved Instances for a 1-year term
- B. All Upfront Reserved Instances for a 1-year term
- C. All Upfront Reserved Instances for a 3-year term
- D. No Upfront Reserved Instances for a 3-year term

Answer(s): C

Reference:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

QUESTION: 206

Which of the following is the responsibility of AWS?

- A. Setting up AWS Identity and Access Management (IAM) users and groups
- B. Physically destroying storage media at end of life
- C. Patching guest operating systems
- D. Configuring security settings on Amazon EC2 instances

Answer(s): B

Explanation:

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

Reference:

<https://aws.amazon.com/compliance/data-center/controls/>

QUESTION: 207

Which of the following is an advantage of using AWS?

- A. AWS audits user data.
- B. Data is automatically secure.
- C. There is no guessing on capacity needs.
- D. AWS manages compliance needs.

Answer(s): C**Explanation:**

AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html>

QUESTION: 208

Which AWS service would a customer use with a static website to achieve lower latency and high transfer speeds?

- A. AWS Lambda
- B. Amazon DynamoDB Accelerator
- C. Amazon Route 53
- D. Amazon CloudFront

Answer(s): D**Explanation:**

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services.

Reference:

<https://aws.amazon.com/cloudfront/>

QUESTION: 209

Which services manage and automate application deployments on AWS? (Choose two.)

- A. AWS Elastic Beanstalk
- B. AWS CodeCommit
- C. AWS Data Pipeline
- D. AWS CloudFormation

E. AWS Config

Answer(s): A, D

Reference:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html>

QUESTION: 210

A user wants guidance on possible savings when migrating from on-premises to AWS. Which tool is suitable for this scenario?

- A. AWS Budgets
- B. Cost Explorer
- C. AWS Total Cost of Ownership (TCO) Calculator
- D. AWS Well-Architected Tool

Answer(s): C

Explanation:

The TCO Calculator provides directional guidance on possible realized savings when deploying AWS. This tool is built on an underlying calculation model, that generates a fair assessment of value that a customer may achieve given the data provided by the user.

Reference:

<https://aws.amazon.com/tco-calculator/>

QUESTION: 211

Which principles are used to architect applications for reliability on the AWS Cloud? (Choose two.)

- A. Design for automated failure recovery
- B. Use multiple Availability Zones
- C. Manage changes via documented processes
- D. Test for moderate demand to ensure reliability
- E. Backup recovery to an on-premises environment

Answer(s): A, B

Reference:

<https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/>

QUESTION: 212

What tasks should a customer perform when that customer suspects an AWS account has been compromised? (Choose two.)

- A. Rotate passwords and access keys.
- B. Remove MFA tokens

- C. Move resources to a different AWS Region.
- D. Delete AWS CloudTrail Resources.
- E. Contact AWS Support.

Answer(s): A, E

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/potential-account-compromise/>

QUESTION: 213

What is an example of high availability in the AWS Cloud?

- A. Consulting AWS technical support at any time day or night
- B. Ensuring an application remains accessible, even if a resource fails
- C. Making any AWS service available for use by paying on demand
- D. Deploying in any part of the world using AWS Regions

Answer(s): B

Reference:

<https://aws.amazon.com/blogs/startups/high-availability-for-mere-mortals/>

QUESTION: 214

Which AWS security service protects applications from distributed denial of service attacks with always-on detection and automatic inline mitigations?

- A. Amazon Inspector
- B. AWS Web Application Firewall (AWS WAF)
- C. Elastic Load Balancing (ELB)
- D. AWS Shield

Answer(s): D

Explanation:

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.

Reference:

<https://aws.amazon.com/shield/>

QUESTION: 215

A company wants to monitor the CPU usage of its Amazon EC2 resources. Which AWS service should the company use?

- A. AWS CloudTrail

- B. Amazon CloudWatch
- C. AWS Cost and Usage report
- D. Amazon Simple Notification Service (Amazon SNS)

Answer(s): B

Explanation:

With Basic monitoring you get data on your cloudwatch metrics every 5 minutes. Enabling detailed monitoring, you will get the data every one minute.

To check if detailed monitoring is enabled, on your EC2 Console, Select the instance, on the lower plane, Select Monitoring.

Reference:

<https://forums.aws.amazon.com/thread.jspa?threadID=263876>

QUESTION: 216

What is an AWS Identity and Access Management (IAM) role?

- A. A user associated with an AWS resource
- B. A group associated with an AWS resource
- C. An entity that defines a set of permissions for use with an AWS resource
- D. An authentication credential associated with a multi-factor authentication (MFA) token

Answer(s): C

Explanation:

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Reference:

<https://aws.amazon.com/iam/>

QUESTION: 217

What are the advantages of Reserved Instances? (Choose two.)

- A. They provide a discount over on-demand pricing.
- B. They provide access to additional instance types.
- C. They provide additional networking capability.
- D. Customers can upgrade instances as new types become available.
- E. Customers can reserve capacity in an Availability Zone.

Answer(s): A, E

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-basics/>

QUESTION: 218

How do Amazon EC2 Auto Scaling groups help achieve high availability for a web application?

- A. They automatically add more instances across multiple AWS Regions based on global demand of the application.
- B. They automatically add or replace instances across multiple Availability Zones when the application needs it.
- C. They enable the application's static content to reside closer to end users.
- D. They are able to distribute incoming requests across a tier of web server instances.

Answer(s): B

Explanation:

When the unhealthy Availability Zone returns to a healthy state, Auto Scaling automatically redistributes the application instances evenly across all of the designated Availability Zones.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html>

QUESTION: 219

How can one AWS account use Reserved Instances from another AWS account?

- A. By using Amazon EC2 Dedicated Instances
- B. By using AWS Organizations consolidated billing
- C. By using the AWS Cost Explorer tool
- D. By using AWS Budgets

Answer(s): B

Explanation:

The account that originally purchased the Reserved Instance receives the discount first. If the purchasing account doesn't have any instances that match the terms of the Reserved Instance, the discount for the Reserved Instance is assigned to any matching usage on another account in the organization.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/>

QUESTION: 220

A customer runs an On-Demand Amazon Linux EC2 instance for 3 hours, 5 minutes, and 6 seconds. For how much time will the customer be billed?

- A. 3 hours, 5 minutes
- B. 3 hours, 5 minutes, and 6 seconds
- C. 3 hours, 6 minutes
- D. 4 hours

Answer(s): B

Reference:

<https://aws.amazon.com/about-aws/whats-new/2017/10/announcing-amazon-ec2-per-second-billing/>

QUESTION: 221

Which of the following AWS services provide compute resources? (Choose two.)

- A. AWS Lambda
- B. Amazon Elastic Container Service (Amazon ECS)
- C. AWS CodeDeploy
- D. Amazon Glacier
- E. AWS Organizations

Answer(s): A, B**Reference:**

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/compute-services.html>

QUESTION: 222

Which AWS service enables users to deploy infrastructure as code by automating the process of provisioning resources?

- A. Amazon GameLift
- B. AWS CloudFormation
- C. AWS Data Pipeline
- D. AWS Glue

Answer(s): B**Explanation:**

AWS CloudFormation provides a common language for you to model and provision AWS and third party application resources in your cloud environment. AWS CloudFormation allows you to use programming languages or 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. This gives you a single source of truth for your AWS and third party resources.

Reference:

<https://aws.amazon.com/cloudformation/>

QUESTION: 223

Which AWS services provide a way to extend an on-premises architecture to the AWS Cloud? (Choose two.)

- A. Amazon EBS
- B. AWS Direct Connect
- C. Amazon CloudFront
- D. AWS Storage Gateway

E. Amazon Connect**Answer(s): B, D****Reference:**<https://aws.amazon.com/hybrid/>**QUESTION: 224**

Which of the following allows users to provision a dedicated network connection from their internal network to AWS?

- A. AWS CloudHSM
- B. AWS Direct Connect
- C. AWS VPN
- D. Amazon Connect

Answer(s): B**Explanation:**

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This allows you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space, while maintaining network separation between the public and private environments. Virtual interfaces can be reconfigured at any time to meet your changing needs.

Reference:<https://aws.amazon.com/directconnect/>**QUESTION: 225**

Which services use AWS edge locations? (Choose two.)

- A. Amazon CloudFront
- B. AWS Shield
- C. Amazon EC2
- D. Amazon RDS
- E. Amazon ElastiCache

Answer(s): A, B**Reference:**<https://www.edureka.co/community/600/what-is-an-edge-location-in-aws>**QUESTION: 226**

Which service would provide network connectivity in a hybrid architecture that includes the AWS Cloud?

- A. Amazon VPC
- B. AWS Direct Connect
- C. AWS Directory Service
- D. Amazon API Gateway

Answer(s): B

Explanation:

Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated, private section of the AWS Cloud to launch resources in a virtual data center in the cloud. Amazon VPC allows you to leverage multiple Availability Zones (AZ) within a region so that you can build greater fault tolerance within your workloads. You have complete control.

Reference:

<https://aws.amazon.com/blogs/publicsector/aws-networking-capabilities-gives-you-choices-for-hybrid-cloud-connectivity-but-which-service-works-best-for-your-use-case/>

QUESTION: 227

Which tool can be used to compare the costs of running a web application in a traditional hosting environment to running it on AWS?

- A. AWS Cost Explorer
- B. AWS Budgets
- C. AWS Cost and Usage report
- D. AWS Total Cost of Ownership (TCO) Calculator

Answer(s): D

Reference:

<https://aws.amazon.com/tco-calculator/>

QUESTION: 228

What is the value of using third-party software from AWS Marketplace instead of installing third-party software on Amazon EC2? (Choose two.)

- A. Users pay for software by the hour or month depending on licensing.
- B. AWS Marketplace enables the user to launch applications with 1-Click.
- C. AWS Marketplace data encryption is managed by a third-party vendor.
- D. AWS Marketplace eliminates the need to upgrade to newer software versions.
- E. Users can deploy third-party software without testing.

Answer(s): A, B

Reference:

<https://aws.amazon.com/partners/aws-marketplace/>

QUESTION: 229

Which of the following is a cloud architectural design principle?

- A. Scale up, not out.
- B. Loosely couple components.
- C. Build monolithic systems.
- D. Use commercial database software.

Answer(s): B

Explanation:

Loosely coupled architectures reduce interdependencies, so that a change or failure in a component does not cascade to other components.

Reference:

https://aws-certified-cloud-practitioner.fandom.com/wiki/1.3_List_the_different_cloud_architecture_design_principles

QUESTION: 230

Under the shared responsibility model; which of the following areas are the customer's responsibility? (Choose two.)

- A. Firmware upgrades of network infrastructure
- B. Patching of operating systems
- C. Patching of the underlying hypervisor
- D. Physical security of data centers
- E. Configuration of the security group

Answer(s): B, E

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 231

Which service enables customers to audit and monitor changes in AWS resources?

- A. AWS Trusted Advisor
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. AWS Config

Answer(s): D

Explanation:

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource

configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Reference:

<https://aws.amazon.com/config/>

QUESTION: 232

Which AWS service identifies security groups that allow unrestricted access to a user's AWS resources?

- A. AWS CloudTrail
- B. AWS Trusted Advisor
- C. Amazon CloudWatch
- D. Amazon Inspector

Answer(s): B

QUESTION: 233

According to the AWS shared responsibility model, who is responsible for configuration management?

- A. It is solely the responsibility of the customer.
- B. It is solely the responsibility of AWS.
- C. It is shared between AWS and the customer.
- D. It is not part of the AWS shared responsibility model.

Answer(s): C

Explanation:

AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 234

Which AWS service is a content delivery network that securely delivers data, video, and applications to users globally with low latency and high speeds?

- A. AWS CloudFormation
- B. AWS Direct Connect
- C. Amazon CloudFront

D. Amazon Pinpoint

Answer(s): C

Explanation:

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services.

Reference:

<https://aws.amazon.com/cloudfront/>

QUESTION: 235

Which benefit of the AWS Cloud supports matching the supply of resources with changing workload demands?

- A. Security
- B. Reliability
- C. Elasticity
- D. High availability

Answer(s): C

Reference:

<https://wa.aws.amazon.com/wat.map.en.html>

QUESTION: 236

A user is running an application on AWS and notices that one or more AWS-owned IP addresses is involved in a distributed denial-of-service (DDoS) attack.

Who should the user contact FIRST about this situation?

- A. AWS Premium Support
- B. AWS Technical Account Manager
- C. AWS Solutions Architect
- D. AWS Abuse team

Answer(s): D

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

QUESTION: 237

Which of the following are benefits of hosting infrastructure in the AWS Cloud? (Choose two.)

- A. There are no upfront commitments.
- B. AWS manages all security in the cloud.
- C. Users have the ability to provision resources on demand.
- D. Users have access to free and unlimited storage.
- E. Users have control over the physical infrastructure.

Answer(s): A, C

QUESTION: 238

What AWS service would be used to centrally manage AWS access policies across multiple accounts?

- A. AWS Service Catalog
- B. AWS Config
- C. AWS Trusted Advisor
- D. AWS Organizations

Answer(s): B

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

QUESTION: 239

What is AWS Trusted Advisor?

- A. It is an AWS staff member who provides recommendations and best practices on how to use AWS.
- B. It is a network of AWS partners who provide recommendations and best practices on how to use AWS.
- C. It is an online tool with a set of automated checks that provides recommendations on cost optimization, performance, and security.
- D. It is another name for AWS Technical Account Managers who provide recommendations on cost optimization, performance, and security.

Answer(s): C

Explanation:

AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices.

Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

QUESTION: 240

Which AWS service or feature allows a company to visualize, understand, and manage AWS costs and usage over time?

- A. AWS Budgets
- B. AWS Cost Explorer
- C. AWS Organizations
- D. Consolidated billing

Answer(s): B

Explanation:

AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time.

Reference:

<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>

QUESTION: 241

Which AWS service offers on-demand access to AWS security and compliance reports?

- A. AWS CloudTrail
- B. AWS Artifact
- C. AWS Health
- D. Amazon CloudWatch

Answer(s): B

Explanation:

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Reference:

<https://aws.amazon.com/artifact/>

QUESTION: 242

What are the benefits of using the AWS Cloud for companies with customers in many countries around the world? (Choose two.)

- A. Companies can deploy applications in multiple AWS Regions to reduce latency.
- B. Amazon Translate automatically translates third-party website interfaces into multiple languages.
- C. Amazon CloudFront has multiple edge locations around the world to reduce latency.

- D. Amazon Comprehend allows users to build applications that can respond to user requests in many languages.
- E. Elastic Load Balancing can distribute application web traffic to multiple AWS Regions around the world, which reduces latency.

Answer(s): A, C

Reference:

<https://aws.amazon.com/comprehend/features/>
<https://aws.amazon.com/cloudfront/>

QUESTION: 243

Which AWS service handles the deployment details of capacity provisioning, load balancing, Auto Scaling, and application health monitoring?

- A. AWS Config
- B. AWS Elastic Beanstalk
- C. Amazon Route 53
- D. Amazon CloudFront

Answer(s): B

Explanation:

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

Reference:

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

QUESTION: 244

Which AWS service provides inbound and outbound network ACLs to harden external connectivity to Amazon EC2?

- A. AWS IAM
- B. Amazon Connect
- C. Amazon VPC
- D. Amazon API Gateway

Answer(s): C

Reference:

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

QUESTION: 245

When a company provisions web servers in multiple AWS Regions, what is being increased?

- A. Coupling
- B. Availability
- C. Security
- D. Durability

Answer(s): B

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

QUESTION: 246

The pay-as-you-go pricing model for AWS services:

- A. reduces capital expenditures.
- B. requires payment up front for AWS services.
- C. is relevant only for Amazon EC2, Amazon S3, and Amazon RDS.
- D. reduces operational expenditures.

Answer(s): A

Reference:

<https://www.10thmagnitude.com/opex-vs-capex-the-real-cloud-computing-cost-advantage/>

QUESTION: 247

Under the AWS shared responsibility model, AWS is responsible for which security-related task?

- A. Lifecycle management of IAM credentials
- B. Physical security of global infrastructure
- C. Encryption of Amazon EBS volumes
- D. Firewall configuration

Answer(s): B

Reference:

<https://cloudacademy.com/blog/aws-shared-responsibility-model-security/>

QUESTION: 248

Which AWS service enables users to consolidate billing across multiple accounts?

- A. Amazon QuickSight
- B. AWS Organizations
- C. AWS Budgets
- D. Amazon Forecast

Answer(s): B

Explanation:

You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. Every organization in AWS Organizations has a master (payer) account that pays the charges of all the member (linked) accounts.

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION: 249

Under the AWS shared responsibility model, which of the following is an example of security in the AWS Cloud?

- A. Managing edge locations
- B. Physical security
- C. Firewall configuration
- D. Global infrastructure

Answer(s): B**Reference:**

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 250

How can an AWS user with an AWS Basic Support plan obtain technical assistance from AWS?

- A. AWS Senior Support Engineers
- B. AWS Technical Account Managers
- C. AWS Trusted Advisor
- D. AWS Discussion Forums

Answer(s): D**Reference:**

<https://aws.amazon.com/premiumsupport/faqs/>

QUESTION: 251

Which of the following are pillars of the AWS Well-Architected Framework? (Choose two.)

- A. Multiple Availability Zones
- B. Performance efficiency
- C. Security
- D. Encryption usage
- E. High availability

Answer(s): B, C**Reference:**

https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf (5)

QUESTION: 252

After selecting an Amazon EC2 Dedicated Host reservation, which pricing option would provide the largest discount?

- A. No upfront payment
- B. Hourly on-demand payment
- C. Partial upfront payment
- D. All upfront payment

Answer(s): D**Reference:**

<https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/>

QUESTION: 253

What is an advantage of deploying an application across multiple Availability Zones?

- A. There is a lower risk of service failure if a natural disaster causes a service disruption in a given AWS Region.
- B. The application will have higher availability because it can withstand a service disruption in one Availability Zone.
- C. There will be better coverage as Availability Zones are geographically distant and can serve a wider area.
- D. There will be decreased application latency that will improve the user experience.

Answer(s): B**Reference:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

QUESTION: 254

A Cloud Practitioner is asked how to estimate the cost of using a new application on AWS. What is the MOST appropriate response?

- A. Inform the user that AWS pricing allows for on-demand pricing.
- B. Direct the user to the AWS Simple Monthly Calculator for an estimate.
- C. Use Amazon QuickSight to analyze current spending on-premises.
- D. Use Amazon AppStream 2.0 for real-time pricing analytics.

Answer(s): B**Reference:**

<https://aws.amazon.com/premiumsupport/knowledge-center/estimating-aws-resource-costs/>

QUESTION: 255

A company wants to migrate its applications to a VPC on AWS. These applications will need to access on-premises resources. What combination of actions will enable the company to accomplish this goal? (Choose two.)

- A. Use the AWS Service Catalog to identify a list of on-premises resources that can be migrated.
- B. Build a VPN connection between an on-premises device and a virtual private gateway in the new VPC.
- C. Use Amazon Athena to query data from the on-premises database servers.
- D. Connect the company's on-premises data center to AWS using AWS Direct Connect.
- E. Leverage Amazon CloudFront to restrict access to static web content provided through the company's on-premises web servers.

Answer(s): B, D

Reference:

<https://aws.amazon.com/blogs/apn/amazon-vpc-for-on-premises-network-engineers-part-one/>

QUESTION: 256

A web application running on AWS has been spammed with malicious requests from a recurring set of IP addresses. Which AWS service can help secure the application and block the malicious traffic?

- A. AWS IAM
- B. Amazon GuardDuty
- C. Amazon Simple Notification Service (Amazon SNS)
- D. AWS WAF

Answer(s): D

Explanation:

AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. You can use AWS WAF to define customizable web security rules that control which traffic accesses your web applications. If you use AWS Shield Advanced, you can use AWS WAF at no extra cost for those protected resources and can engage the DRT to create WAF rules.

Reference:

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

QUESTION: 257

Treating infrastructure as code in the AWS Cloud allows users to:

- A. automate migration of on-premises hardware to AWS data centers.
- B. let a third party automate an audit of the AWS infrastructure.
- C. turn over application code to AWS so it can run on the AWS infrastructure

D. automate the infrastructure provisioning process.

Answer(s): D

Reference:

<https://asperbrothers.com/blog/infrastructure-as-code-aws/>

QUESTION: 258

A company requires a dedicated network connection between its on-premises servers and the AWS Cloud. Which AWS service should be used?

- A. AWS VPN
- B. AWS Direct Connect
- C. Amazon API Gateway
- D. Amazon Connect

Answer(s): B

Explanation:

You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you with a private, high bandwidth network connection between your network and your VPC. With multiple virtual interfaces, you can even establish private connectivity to multiple VPCs while maintaining network isolation.

Reference:

<https://aws.amazon.com/directconnect/>

QUESTION: 259

Which AWS service can be used to query stored datasets directly from Amazon S3 using standard SQL?

- A. AWS Glue
- B. AWS Data Pipeline
- C. Amazon CloudSearch
- D. Amazon Athena

Answer(s): D

Explanation:

Amazon Athena is defined as “an interactive query service that makes it easy to analyse data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL.” So, it’s another SQL query engine for large data sets stored in S3. This is very similar to other SQL query engines, such as Apache Drill. But unlike Apache Drill, Athena is limited to data only from Amazon’s own S3 storage service. However, Athena is able to query a variety of file formats, including, but not limited to CSV, Parquet, JSON, etc.

QUESTION: 260

AWS CloudFormation is designed to help the user:

- A. model and provision resources
- B. update application code
- C. set up data lakes.
- D. create reports for billing.

Answer(s): A

Explanation:

AWS CloudFormation provides a common language for you to model and provision AWS and third party application resources in your cloud environment. AWS CloudFormation allows you to use programming languages or 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. This gives you a single source of truth for your AWS and third party resources.

Reference:

<https://aws.amazon.com/cloudformation/>

QUESTION: 261

Which of the following is an AWS database service?

- A. Amazon Redshift
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon S3 Glacier
- D. AWS Snowball

Answer(s): A

Reference:

<https://www.sisense.com/glossary/redshift-database/>

QUESTION: 262

A Cloud Practitioner must determine if any security groups in an AWS account have been provisioned to allow unrestricted access for specific ports. What is the SIMPLEST way to do this?

- A. Review the inbound rules for each security group in the Amazon EC2 management console to check for port 0.0.0.0/0.
- B. Run AWS Trusted Advisor and review the findings.
- C. Open the AWS IAM console and check the inbound rule filters for open access.
- D. In AWS Config, create a custom rule that invokes an AWS Lambda function to review rules for inbound access.

Answer(s): B

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-security-groups.html>

QUESTION: 263

What are the benefits of developing and running a new application in the AWS Cloud compared to on-premises? (Choose two.)

- A. AWS automatically distributes the data globally for higher durability.
- B. AWS will take care of operating the application.
- C. AWS makes it easy to architect for high availability.
- D. AWS can easily accommodate application demand changes.
- E. AWS takes care of application security patching.

Answer(s): C, D

QUESTION: 264

A user needs an automated security assessment report that will identify unintended network access to Amazon EC2 instances and vulnerabilities on those instances. Which AWS service will provide this assessment report?

- A. EC2 security groups
- B. AWS Config
- C. Amazon Macie
- D. Amazon Inspector

Answer(s): D

Explanation:

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Reference:

<https://aws.amazon.com/inspector/>

QUESTION: 265

How can a company isolate the costs of production and non-production workloads on AWS?

- A. Create Identity and Access Management (IAM) roles for production and non-production workloads
- B. Use different accounts for production and non-production expenses.
- C. Use Amazon EC2 for non-production workloads and other services for production workloads.
- D. Use Amazon CloudWatch to monitor the use of services.

Answer(s): B

Reference:

<https://aws.amazon.com/answers/account-management/aws-multi-account-billing-strategy/>

QUESTION: 266

Where can users find a catalog of AWS-recognized providers of third-party security solutions?

- A. AWS Service Catalog
- B. AWS Marketplace
- C. AWS Quick Start
- D. AWS CodeDeploy

Answer(s): A

Explanation:

AWS Service Catalog Delivery Partners are APN Consulting Partners who help create catalogs of IT services that are approved by the customer's organization for use on AWS. With AWS Service Catalog, customers and partners can centrally manage commonly deployed IT services to help achieve consistent governance and meet compliance requirements while enabling users to self-provision approved services.

Reference:

<https://aws.amazon.com/servicecatalog/partners/>

QUESTION: 267

A Cloud Practitioner needs to store data for 7 years to meet regulatory requirements. Which AWS service will meet this requirement at the LOWEST cost?

- A. Amazon S3
- B. AWS Snowball
- C. Amazon Redshift
- D. Amazon S3 Glacier

Answer(s): D

Explanation:

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases, and is a cost-effective and easy-to-manage alternative to magnetic tape systems, whether they are on-premises libraries or off-premises services.

Reference:

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

QUESTION: 268

What are the immediate benefits of using the AWS Cloud? (Choose two.)

- A. Increased IT staff
- B. Capital expenses are replaced with variable expenses.
- C. User control of infrastructure.
- D. Increased agility.
- E. AWS holds responsibility for security in the cloud.

Answer(s): C, D

QUESTION: 269

Which security service automatically recognizes and classifies sensitive data or intellectual property on AWS?

- A. Amazon GuardDuty
- B. Amazon Macie
- C. Amazon Inspector
- D. AWS Shield

Answer(s): B

Explanation:

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property. It provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.

Reference:

<https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html>

QUESTION: 270

What is the purpose of AWS Storage Gateway?

- A. It ensures on-premises data storage is 99.99999999% durable.
- B. It transports petabytes of data to and from AWS.
- C. It connects to multiple Amazon EC2 instances.
- D. It connects on-premises data storage to the AWS Cloud.

Answer(s): D

Explanation:

Moving data to the cloud is not quite as simple as flipping a switch. For companies that have managed their own data centers or server rooms for decades, there are a few steps to consider -- and it's not always wise to pull the plug on an internal infrastructure quite so quickly. If a startup uses on-premise business servers and then experiences unexpected growth, abandoning those servers doesn't make sense (even if the long-term plan is to do exactly that).

AWS Storage Gateway is a way to bridge this gap for companies of any size. It's a hybrid storage option that connects on-premise storage including age-old tape backup systems to the cloud in a way that also provides one console to access all storage configurations.

Reference:

<https://www.techradar.com/news/what-is-aws-storage-gateway>

QUESTION: 271

What should users do if they want to install an application in geographically isolated locations?

- A. Install the application using multiple internet gateways.
- B. Deploy the application to an Amazon VPC.
- C. Deploy the application to multiple AWS Regions.
- D. Configure the application using multiple NAT gateways.

Answer(s): C

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

QUESTION: 272

A system in the AWS Cloud is designed to withstand the failure of one or more components.

What is this an example of?

- A. Elasticity
- B. High Availability
- C. Scalability
- D. Agility

Answer(s): B

Reference:

https://wa.aws.amazon.com/wat.question.REL_7.en.html

QUESTION: 273

A Cloud Practitioner needs a consistent and dedicated connection between AWS resources and an on-premises system. Which AWS service can fulfill this requirement?

- A. AWS Direct Connect
- B. AWS VPN
- C. Amazon Connect
- D. AWS Data Pipeline

Answer(s): A

Explanation:

You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you with a private, high bandwidth network

connection between your network and your VPC. With multiple virtual interfaces, you can even establish private connectivity to multiple VPCs while maintaining network isolation.

Reference:

<https://aws.amazon.com/directconnect/>

QUESTION: 274

Within the AWS shared responsibility model, who is responsible for security and compliance?

- A. The customer is responsible.
- B. AWS is responsible.
- C. AWS and the customer share responsibility.
- D. AWS shares responsibility with the relevant governing body.

Answer(s): C**Explanation:**

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 275

To use the AWS CLI, users are required to generate:

- A. a password policy
- B. an access/secret key
- C. a managed policy
- D. an API key

Answer(s): B**QUESTION: 276**

Which AWS service is used to provide encryption for Amazon EBS?

- A. AWS Certificate Manager
- B. AWS Systems Manager
- C. AWS KMS
- D. AWS Config

Answer(s): C**Reference:**

<https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

QUESTION: 277

How does AWS charge for AWS Lambda usage once the free tier has been exceeded?
(Choose two.)

- A. By the time it takes for the Lambda function to execute.
- B. By the number of versions of a specific Lambda function.
- C. By the number of requests made for a given Lambda function.
- D. By the programming language that is used for the Lambda function.
- E. By the total number of Lambda functions in an AWS account.

Answer(s): A, C

QUESTION: 278

Which of the following describes the relationships among AWS Regions, Availability Zones, and edge locations? (Choose two.)

- A. There are more AWS Regions than Availability Zones.
- B. There are more edge locations than AWS Regions.
- C. An edge location is an Availability Zone.
- D. There are more AWS Regions than edge locations.
- E. There are more Availability Zones than AWS Regions.

Answer(s): B, E

QUESTION: 279

What does AWS Shield Standard provide?

- A. WAF rules
- B. DDoS protection
- C. Identity and Access Management (IAM) permissions and access to resources
- D. Data encryption

Answer(s): B

Explanation:

AWS Shield Standard provides protection for all AWS customers from common, most frequently occurring network and transport layer DDoS attacks that target your web site or application at no additional charge.

Reference:

<https://aws.amazon.com/shield/pricing/>

QUESTION: 280

A company wants to build its new application workloads in the AWS Cloud instead of using on-premises resources. What expense can be reduced using the AWS Cloud?

- A. The cost of writing custom-built Java or Node.js code
- B. Penetration testing for security
- C. hardware required to support new applications
- D. Writing specific test cases for third-party applications.

Answer(s): C

Reference:

<https://aws.amazon.com/pricing/cost-optimization/>

QUESTION: 281

What does AWS Marketplace allow users to do? (Choose two.)

- A. Sell unused Amazon EC2 Spot Instances.
- B. Sell solutions to other AWS users.
- C. Buy third-party software that runs on AWS.
- D. Purchase AWS security and compliance documents.
- E. Order AWS Snowball.

Answer(s): B, C

Reference:

<https://aws.amazon.com/marketplace>

QUESTION: 282

What does it mean if a user deploys a hybrid cloud architecture on AWS?

- A. All resources run using on-premises infrastructure.
- B. Some resources run on-premises and some run in a colocation center.
- C. All resources run in the AWS Cloud.
- D. Some resources run on-premises and some run in the AWS Cloud.

Answer(s): D

Reference:

<https://aws.amazon.com/hybrid/>

QUESTION: 283

Which AWS service allows users to identify the changes made to a resource over time?

- A. Amazon Inspector
- B. AWS Config
- C. AWS Service Catalog
- D. AWS IAM

Answer(s): B

Reference:

<https://docs.aws.amazon.com/config/latest/developerguide/view-manage-resource.html>

QUESTION: 284

How can a company reduce its Total Cost of Ownership (TCO) using AWS?

- A. By minimizing large capital expenditures
- B. By having no responsibility for third-party license costs
- C. By having no operational expenditures
- D. By having AWS manage applications

Answer(s): A

Explanation:

AWS helps you reduce Total Cost of Ownership (TCO) by reducing the need to invest in large capital expenditures and providing a pay-as-you-go model that empowers you to invest in the capacity you need and use it only when the business requires it.

Reference:

<https://aws.amazon.com/tco-calculator/>

QUESTION: 285

Which activity is a customer responsibility in the AWS Cloud according to the AWS shared responsibility model?

- A. Ensuring network connectivity from AWS to the internet
- B. Patching and fixing flaws within the AWS Cloud infrastructure
- C. Ensuring the physical security of cloud data centers
- D. Ensuring Amazon EBS volumes are backed up

Answer(s): D

Reference:

<https://aws.amazon.com/blogs/security/the-aws-shared-responsibility-model-and-gdpr/>

QUESTION: 286

What are the advantages of the AWS Cloud? (Choose two.)

- A. Fixed rate monthly cost
- B. No need to guess capacity requirements
- C. Increased speed to market
- D. Increased upfront capital expenditure
- E. Physical access to cloud data centers

Answer(s): B, C

Reference:

<https://data-flair.training/blogs/aws-advantages/>

QUESTION: 287

When comparing the total cost of ownership (TCO) of an on-premises infrastructure to a cloud architecture, what costs should be considered? (Choose two.)

- A. The credit card processing fees for application transactions in the cloud.
- B. The cost of purchasing and installing server hardware in the on-premises data.
- C. The cost of administering the infrastructure, including operating system and software installations, patches, backups, and recovering from failures.
- D. The costs of third-party penetration testing.
- E. The advertising costs associated with an ongoing enterprise-wide campaign.

Answer(s): B, C**Reference:**

<https://aws.amazon.com/tco-calculator/>

QUESTION: 288

Which AWS feature allows a company to take advantage of usage tiers for services across multiple member accounts?

- A. Service control policies (SCPs)
- B. Consolidated billing
- C. All Upfront Reserved Instances
- D. AWS Cost Explorer

Answer(s): B**Reference:**

<https://aws.amazon.com/tco-calculator/>

QUESTION: 289

What is one of the customer's responsibilities according to the AWS shared responsibility model?

- A. Virtualization infrastructure
- B. Network infrastructure
- C. Application security
- D. Physical security of hardware

Answer(s): C**Reference:**

<https://cloudacademy.com/blog/aws-shared-responsibility-model-security/>

QUESTION: 290

What helps a company provide a lower latency experience to its users globally?

- A. Using an AWS Region that is central to all users
- B. Using a second Availability Zone in the AWS Region that is being used
- C. Enabling caching in the AWS Region that is being used
- D. Using edge locations to put content closer to all users

Answer(s): A

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html>

QUESTION: 291

How can the AWS Cloud increase user workforce productivity after migration from an on-premises data center?

- A. Users do not have to wait for infrastructure provisioning.
- B. The AWS Cloud infrastructure is much faster than an on-premises data center infrastructure.
- C. AWS takes over application configuration management on behalf of users.
- D. Users do not need to address security and compliance issues.

Answer(s): A

Reference:

<https://d1.awsstatic.com/whitepapers/Migration/aws-migration-whitepaper.pdf>

QUESTION: 292

Which AWS service provides a quick and automated way to create and manage AWS accounts?

- A. AWS QuickSight
- B. Amazon Lightsail
- C. AWS Organizations
- D. Amazon Connect

Answer(s): C

Reference:

<https://aws.amazon.com/blogs/mt/automate-account-creation-and-resource-provisioning-using-aws-service-catalog-aws-organizations-and-aws-lambda/>

QUESTION: 293

Which Amazon RDS feature can be used to achieve high availability?

- A. Multiple Availability Zones
- B. Amazon Reserved Instances
- C. Provisioned IOPS storage
- D. Enhanced monitoring

Answer(s): A

Explanation:

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

Reference:

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

QUESTION: 294

Where should users report that AWS resources are being used for malicious purposes?

- A. AWS Abuse team
- B. AWS Shield
- C. AWS Support
- D. AWS Developer Forums

Answer(s): A

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

QUESTION: 295

Which AWS service needs to be enabled to track all user account changes within the AWS Management Console?

- A. AWS CloudTrail
- B. Amazon Simple Notification Service (Amazon SNS)
- C. VPC Flow Logs
- D. AWS CloudHSM

Answer(s): A

Explanation:

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

Reference:

<https://aws.amazon.com/cloudtrail/>

QUESTION: 296

What is an AWS Cloud design best practice?

- A. Tight coupling of components
- B. Single point of failure
- C. High availability
- D. Overprovisioning of resources

Answer(s): C

QUESTION: 297

Which of the following is an example of how moving to the AWS Cloud reduces upfront cost?

- A. By replacing large variable costs with lower capital investments
- B. By replacing large capital investments with lower variable costs
- C. By allowing the provisioning of compute and storage at a fixed level to meet peak demand
- D. By replacing the repeated scaling of virtual servers with a simpler fixed-scale model

Answer(s): B

Explanation:

AWS does not require minimum spend commitments or long-term contracts. You replace large upfront expenses with low variable payments that only apply to what you use. With AWS you are not bound to multi-year agreements or complicated licensing models.

Reference:

<https://aws.amazon.com/economics/>

QUESTION: 298

When designing a typical three-tier web application, which AWS services and/or features improve availability and reduce the impact failures? (Choose two.)

- A. AWS Auto Scaling for Amazon EC2 instances
- B. Amazon VPC subnet ACLs to check the health of a service
- C. Distributed resources across multiple Availability Zones
- D. AWS Server Migration Service (AWS SMS) to move Amazon EC2 instances into a different Region
- E. Distributed resources across multiple AWS points of presence

Answer(s): A, C

Reference:

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

QUESTION: 299

Which cloud design principle aligns with AWS Cloud best practices?

- A. Create fixed dependencies among application components
- B. Aggregate services on a single instance
- C. Deploy applications in a single Availability Zone
- D. Distribute the compute load across multiple resources

Answer(s): D

Explanation:

Use load balancing for offloading encryption termination (TLS) to improve performance and to manage and route traffic effectively. Distribute traffic across multiple resources or services to allow your workload to take advantage of the elasticity that AWS provides.

Reference:

https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

QUESTION: 300

Which of the following are recommended practices for managing IAM users? (Choose two.)

- A. Require IAM users to change their passwords after a specified period of time
- B. Prevent IAM users from reusing previous passwords
- C. Recommend that the same password be used on AWS and other sites
- D. Require IAM users to store their passwords in raw text
- E. Disable multi-factor authentication (MFA) for IAM users

Answer(s): A, B

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

QUESTION: 301

A company is migrating from on-premises data centers to the AWS Cloud and is looking for hands-on help with the project. How can the company get this support? (Choose two.)

- A. Ask for a quote from the AWS Marketplace team to perform a migration into the company's AWS account.
- B. Contact AWS Support and open a case for assistance
- C. Use AWS Professional Services to provide guidance and to set up an AWS Landing Zone in the company's AWS account
- D. Select a partner from the AWS Partner Network (APN) to assist with the migration
- E. Use Amazon Connect to create a new request for proposal (RFP) for expert assistance in migrating to the AWS Cloud.

Answer(s): C, D

Reference:

<https://aws.amazon.com/solutions/aws-landing-zone/>

QUESTION: 302

How does the AWS Enterprise Support Concierge team help users?

- A. Supporting application development
- B. Providing architecture guidance
- C. Answering billing and account inquiries
- D. Answering questions regarding technical support cases

Answer(s): C

Reference:

<https://aws.amazon.com/premiumsupport/plans/enterprise/>

QUESTION: 303

An application designed to span multiple Availability Zones is described as:

- A. being highly available
- B. having global reach
- C. using an economy of scale
- D. having elasticity

Answer(s): A

Reference:

https://books.google.com.pk/books?id=IueWBQAAQBAJ&pg=PA11&lpg=PA11&dq=aws+application+designed+to+span+multiple+Availability+Zones+is+described+as+economy+of+scale&source=bl&ots=cj_NsIAxm2&sig=ACfU3U2fe5KOugmORbAoV9lgj_eCGIsItA&hl=en&sa=X&ved=2ahU KEwiGzf-rtbroAhVkxoUKHRhjC-IQ6AEwCnoECAkQAQ#v=onepage&q=aws%20application%20designed%20to%20span%20multiple%20Availability%20Zones%20is%20described%20as%20economy%20of%20scale&f=false

QUESTION: 304

A new service using AWS must be highly available. Yet, due to regulatory requirements, all of its Amazon EC2 instances must be located in a single geographic area. According to best practices, to meet these requirements, the EC2 instances must be placed in at least two:

- A. AWS Regions
- B. Availability Zones
- C. subnets
- D. placement groups

Answer(s): B

Reference:

<https://aws.amazon.com/ec2/faqs/>

QUESTION: 305

Which AWS tool is used to compare the cost of running an application on-premises to running the application in the AWS Cloud?

- A. AWS Trusted Advisor
- B. AWS Simple Monthly Calculator
- C. AWS Total Cost of Ownership (TCO) Calculator
- D. Cost Explorer

Answer(s): C

Reference:

<https://aws.amazon.com/tco-calculator/>

QUESTION: 306

A company has multiple AWS accounts within AWS Organizations and wants to apply the Amazon EC2 Reserved Instances benefit to a single account only. Which action should be taken?

- A. Purchase the Reserved Instances from master payer account and turn off Reserved Instance sharing.
- B. Enable billing alerts in the AWS Billing and Cost Management console.
- C. Purchase the Reserved Instances in individual linked accounts and turn off Reserved Instance sharing from the payer level.
- D. Enable Reserved Instance sharing in the AWS Billing and Cost Management console.

Answer(s): A

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/>

QUESTION: 307

Which situation should be reported to the AWS Abuse team?

- A. In Availability Zone has a service disruption
- B. An intrusion attempt is made from an AWS IP address
- C. A user has trouble accessing an Amazon S3 bucket from an AWS IP address
- D. A user needs to change payment methods due to a compromise

Answer(s): B

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

QUESTION: 308

A company is planning to launch an ecommerce site in a single AWS Region to a worldwide user base.

Which AWS services will allow the company to reach users and provide low latency and high transfer speeds? (Choose two.)

- A. Application Load Balancer
- B. AWS Global Accelerator
- C. AWS Direct Connect
- D. Amazon CloudFront
- E. AWS Lambda

Answer(s): B, D

Reference:

<https://aws.amazon.com/cloudfront/faqs/>

QUESTION: 309

Which AWS service or resource is serverless?

- A. AWS Lambda
- B. Amazon EC2 instances
- C. Amazon Lightsail
- D. Amazon ElastiCache

Answer(s): A

Reference:

<https://blogs.itemis.com/en/serverless-services-on-aws>

QUESTION: 310

Which of the following are components of Amazon VPC? (Choose two.)

- A. Objects
- B. Subnets
- C. Buckets
- D. Internet gateways
- E. Access key

Answer(s): B, D

Reference:

https://subscription.packtpub.com/book/virtualization_and_cloud/9781788293723/3/ch03lvl1sec26/vpc-components

QUESTION: 311

AWS Budgets can be used to:

- A. prevent a given user from creating a resource
- B. send an alert when the utilization of Reserved Instances drops below a certain percentage
- C. set resource limits in AWS accounts to prevent overspending
- D. split an AWS bill across multiple forms of payment

Answer(s): C

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html>

QUESTION: 312

Which of the following will enhance the security of access to the AWS Management Console?
(Choose two.)

- A. AWS Secrets Manager
- B. AWS Certificate Manager
- C. AWS Multi-Factor Authentication (AWS MFA)
- D. Security groups
- E. Password policies

Answer(s): C, E

Reference:

<https://aws.amazon.com/blogs/security/guidelines-for-protecting-your-aws-account-while-using-programmatic-access/>

QUESTION: 313

The AWS Trusted Advisor checks include recommendations regarding which of the following?
(Choose two.)

- A. Information on Amazon S3 bucket permissions
- B. AWS service outages
- C. Multi-factor authentication enabled on the AWS account root user
- D. Available software patches
- E. Number of users in the account

Answer(s): A, C

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/>

QUESTION: 314

Which functions can users perform using AWS KMS?

- A. Create and manage AWS access keys for the AWS account root user
- B. Create and manage AWS access keys for an AWS account IAM user
- C. Create and manage keys for encryption and decryption of data

D. Create and manage keys for multi-factor authentication

Answer(s): C

Reference:

<https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html>

QUESTION: 315

How does AWS Trusted Advisor provide guidance to users of the AWS Cloud? (Choose two.)

- A. It identifies software vulnerabilities in applications running on AWS
- B. It provides a list of cost optimization recommendations based on current AWS usage
- C. It detects potential security vulnerabilities caused by permissions settings on account resources
- D. It automatically corrects potential security issues caused by permissions settings on account resources
- E. It provides proactive alerting whenever an Amazon EC2 instance has been compromised

Answer(s): B, C

QUESTION: 316

Which of the following are advantages of the AWS Cloud? (Choose two.)

- A. AWS manages the maintenance of the cloud infrastructure
- B. AWS manages the security of applications built on AWS
- C. AWS manages capacity planning for physical servers
- D. AWS manages the development of applications on AWS
- E. AWS manages cost planning for virtual servers

Answer(s): A, C

Reference:

<https://aws.amazon.com/compliance/data-center/controls/>

QUESTION: 317

A user deploys an Amazon RDS DB instance in multiple Availability Zones. This strategy involves which pillar of the AWS Well-Architected Framework?

- A. Performance efficiency
- B. Reliability
- C. Cost optimization
- D. Security

Answer(s): B

Reference:

<https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/>

QUESTION: 318

Which AWS services provide a user with connectivity between the AWS Cloud and on-premises resources? (Choose two.)

- A. AWS VPN
- B. Amazon Connect
- C. Amazon Cognito
- D. AWS Direct Connect
- E. AWS Managed Services

Answer(s): A, D

Reference:

<https://aws.amazon.com/directconnect/>

<https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-client-vpn-to-securely-access-aws-and-on-premises-resources/>

QUESTION: 319

Which AWS service is used to pay AWS bills, and monitor usage and budget costs?

- A. AWS Billing and Cost Management
- B. Consolidated billing
- C. Amazon CloudWatch
- D. Amazon QuickSight

Answer(s): A

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html>

QUESTION: 320

Which element of the AWS global infrastructure consists of one or more discrete data centers, each with redundant power, networking, and connectivity, which are housed in separate facilities?

- A. AWS Regions
- B. Availability Zones
- C. Edge locations
- D. Amazon CloudFront

Answer(s): B

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/global-infrastructure.html>

QUESTION: 321

Which Amazon VPC feature enables users to capture information about the IP traffic that reaches Amazon EC2 instances?

- A. Security groups
- B. Elastic network interfaces
- C. Network ACLs
- D. VPC Flow Logs

Answer(s): D

Explanation:

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

Reference:

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

QUESTION: 322

Which AWS service can be used to automatically scale an application up and down without making capacity planning decisions?

- A. Amazon AutoScaling
- B. Amazon Redshift
- C. AWS CloudTrail
- D. AWS Lambda

Answer(s): D

Reference:

<https://aws.amazon.com/blogs/aws/category/auto-scaling/>

QUESTION: 323

AWS Enterprise Support users have access to which service or feature that is not available to users with other AWS Support plans?

- A. AWS Trusted Advisor
- B. AWS Support case
- C. Concierge team
- D. Amazon Connect

Answer(s): C

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

QUESTION: 324

A company wants to migrate a MySQL database to AWS but does not have the budget for Database Administrators to handle routine tasks including provisioning, patching, and performing backups.

Which AWS service will support this use case?

- A. Amazon RDS
- B. Amazon DynamoDB
- C. Amazon DocumentDB
- D. Amazon ElastiCache

Answer(s): A

Explanation:

Amazon RDS makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks, such as hardware provisioning, database setup, patching, and backups. It frees you to focus on your applications, so you can give them the fast performance, high availability, security, and compatibility that they need.

Reference:

<https://aws.amazon.com/blogs/database/part-1-role-of-the-dba-when-moving-to-amazon-rds-responsibilities/>

QUESTION: 325

A company wants to expand from one AWS Region into a second AWS Region. What does the company need to do to start supporting the new Region?

- A. Contact an AWS Account Manager to sign a new contract
- B. Move an Availability Zone to the new Region
- C. Begin deploying resources in the second Region
- D. Download the AWS Management Console for the new Region

Answer(s): C

Reference:

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-region.html>

QUESTION: 326

A user must meet compliance and software licensing requirements that state a workload must be hosted on a physical server. Which Amazon EC2 instance pricing option will meet these requirements?

- A. Dedicated Hosts
- B. Dedicated Instances
- C. Spot Instances
- D. Reserved Instances

Answer(s): A

Reference:

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

QUESTION: 327

Which AWS service will provide a way to generate encryption keys that can be used to encrypt data? (Choose two.)

- A. Amazon Macie
- B. AWS Certificate Manager
- C. AWS Key Management Service (AWS KMS)
- D. AWS Secrets Manager
- E. AWS CloudHSM

Answer(s): C, E

Reference:

<https://docs.aws.amazon.com/crypto/latest/ug/aws-crypt-service-hsm.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

QUESTION: 328

A company is planning to migrate from on-premises to the AWS Cloud.

Which AWS tool or service provides detailed reports on estimated cost savings after migration?

- A. AWS Total Cost of Ownership (TCO) Calculator
- B. Cost Explorer
- C. AWS Budgets
- D. AWS Migration Hub

Answer(s): A

Reference:

<https://docs.aws.amazon.com/migrationhub/latest/ug/hub-api.pdf> (26)

QUESTION: 329

What can assist in evaluating an application for migration to the cloud? (Choose two.)

- A. AWS Trusted Advisor
- B. AWS Professional Services
- C. AWS Systems Manager
- D. AWS Partner Network (APN)
- E. AWS Secrets Manager

Answer(s): B, D

QUESTION: 330

Which AWS service helps users meet contractual and regulatory compliance requirements for data security by using dedicated hardware appliances within the AWS Cloud?

- A. AWS Secrets Manager
- B. AWS CloudHSM
- C. AWS Key Management Service (AWS KMS)
- D. AWS Directory Service

Answer(s): B

Explanation:

The AWS CloudHSM service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are designed and validated to government standards for secure key management. CloudHSM allows you to securely generate, store, and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

Reference:

<https://aws.amazon.com/cloudhsm/faqs/>

QUESTION: 331

Under the AWS shared responsibility model, the customer manages which of the following? (Choose two.)

- A. Decommissioning of physical storage devices
- B. Security group and ACL configuration
- C. Patch management of an Amazon RDS instance operating system
- D. Controlling physical access to data centers
- E. Patch management of an Amazon EC2 instance operating system

Answer(s): B, E

Explanation:

Reference:

<https://www.whizlabs.com/blog/aws-security-shared-responsibility/>

QUESTION: 332

Which AWS service is suitable for an event-driven workload?

- A. Amazon EC2
- B. AWS Elastic Beanstalk
- C. AWS Lambda

D. Amazon Lumberyard

Answer(s): C

Explanation:

An easy-to-use service for deploying and scaling web applications and web services developed in a number of programming languages. You can configure event notifications for your Elastic Beanstalk environment so that notable events can be automatically published to an SNS topic, then pushed to topic subscribers. As an example, you may use this event-driven architecture to coordinate your continuous integration pipeline (such as Jenkins CI). That way, whenever an environment is created, Elastic Beanstalk publishes this event to an SNS topic, which triggers a subscribing Lambda function, which then kicks off a CI job against your newly created Elastic Beanstalk environment.

Reference:

<https://aws.amazon.com/blogs/compute/event-driven-computing-with-amazon-sns-compute-storage-database-and-networking-services/>

QUESTION: 333

What is a value proposition of the AWS Cloud?

- A. AWS is responsible for security in the AWS Cloud
- B. No long-term contract is required
- C. Provision new servers in days
- D. AWS manages user applications in the AWS Cloud

Answer(s): B

Reference:

<https://d1.awsstatic.com/whitepapers/aws-whitepaper-business-value-of-aws.pdf>

QUESTION: 334

What is a characteristic of Amazon S3 cross-region replication?

- A. Both source and destination S3 buckets must have versioning disabled
- B. The source and destination S3 buckets cannot be in different AWS Regions
- C. S3 buckets configured for cross-region replication can be owned by a single AWS account or by different accounts
- D. The source S3 bucket owner must have the source and destination AWS Regions disabled for their account

Answer(s): C

Reference:

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

QUESTION: 335

What is a user responsible for when running an application in the AWS Cloud?

- A. Managing physical hardware
- B. Updating the underlying hypervisor
- C. Providing a list of users approved for data center access
- D. Managing application software updates

Answer(s): D

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 336

A company that does business online needs to quickly deliver new functionality in an iterative manner, minimizing the time to market. Which AWS Cloud feature can provide this?

- A. Elasticity
- B. High availability
- C. Agility
- D. Reliability

Answer(s): C

Reference:

<https://aws.amazon.com/devops/partner-solutions/>

QUESTION: 337

Which features or services can be used to monitor costs and expenses for an AWS account? (Choose two.)

- A. AWS Cost and Usage report
- B. AWS product pages
- C. AWS Simple Monthly Calculator
- D. Billing alerts and Amazon CloudWatch alarms
- E. AWS Price List API

Answer(s): A, D

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charges_with_cloudwatch.html

QUESTION: 338

Amazon Route 53 enables users to:

- A. encrypt data in transit
- B. register DNS domain names

- C. generate and manage SSL certificates
- D. establish a dedicated network connection to AWS

Answer(s): B

Reference:

[**QUESTION: 339**](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide>Welcome.html</p></div><div data-bbox=)

Which AWS service helps identify malicious or unauthorized activities in AWS accounts and workloads?

- A. Amazon Rekognition
- B. AWS Trusted Advisor
- C. Amazon GuardDuty
- D. Amazon CloudWatch

Answer(s): C

Reference:

<https://aws.amazon.com/guardduty/>

QUESTION: 340

A company wants to try a third-party ecommerce solution before deciding to use it long term. Which AWS service or tool will support this effort?

- A. AWS Marketplace
- B. AWS Partner Network (APN)
- C. AWS Managed Services
- D. AWS Service Catalog

Answer(s): A

Reference:

<https://aws.amazon.com/about-aws/whats-new/2019/09/aws-marketplace-easier-to-find-solutions-from-aws-console/>

QUESTION: 341

Which AWS service is a managed NoSQL database?

- A. Amazon Redshift
- B. Amazon DynamoDB
- C. Amazon Aurora
- D. Amazon RDS for MariaDB

Answer(s): B

Reference:

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

QUESTION: 342

Which AWS service should be used to create a billing alarm?

- A. AWS Trusted Advisor
- B. AWS CloudTrail
- C. Amazon CloudWatch
- D. Amazon QuickSight

Answer(s): C

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charges_with_cloudwatch.html

QUESTION: 343

A company is hosting a web application in a Docker container on Amazon EC2. AWS is responsible for which of the following tasks?

- A. Scaling the web application and services developed with Docker
- B. Provisioning or scheduling containers to run on clusters and maintain their availability
- C. Performing hardware maintenance in the AWS facilities that run the AWS Cloud
- D. Managing the guest operating system, including updates and security patches

Answer(s): C

Reference:

<https://aws.amazon.com/getting-started/tutorials/deploy-docker-containers/>

QUESTION: 344

Users are reporting latency when connecting to a website with a global customer base. Which AWS service will improve the customer experience by reducing latency?

- A. Amazon CloudFront
- B. AWS Direct Connect
- C. Amazon EC2 Auto Scaling
- D. AWS Transit Gateway

Answer(s): A

Reference:

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

QUESTION: 345

Which actions represent best practices for using AWS IAM? (Choose two.)

- A. Configure a strong password policy
- B. Share the security credentials among users of AWS accounts who are in the same Region
- C. Use access keys to log in to the AWS Management Console
- D. Rotate access keys on a regular basis
- E. Avoid using IAM roles to delegate permissions

Answer(s): A, D

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

QUESTION: 346

Which AWS feature or service can be used to capture information about incoming and outgoing traffic in an AWS VPC infrastructure?

- A. AWS Config
- B. VPC Flow Logs
- C. AWS Trusted Advisor
- D. AWS CloudTrail

Answer(s): B

Reference:

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

QUESTION: 347

A company wants to use an AWS service to monitor the health of application endpoints, with the ability to route traffic to healthy regional endpoints to improve application availability. Which service will support these requirements?

- A. Amazon Inspector
- B. Amazon CloudWatch
- C. AWS Global Accelerator
- D. Amazon CloudFront

Answer(s): C

Explanation:

AWS Global Accelerator uses the AWS global network to optimize the path from your users to your applications, improving the performance of your traffic by as much as 60%. AWS Global Accelerator continually monitors the health of your application endpoints and redirects traffic to healthy endpoints in less than 30 seconds.

Reference:

<https://aws.amazon.com/global-accelerator/?blogs-global-accelerator.sort-by=item.additionalFields.createdDate&blogs-global-accelerator.sort-order=desc&aws-global->

accelerator-wn.sort-by=item.additionalFields.postDateTime&aws-global-accelerator-wn.sort-order=desc

QUESTION: 348

According to the AWS Well-Architected Framework, what change management steps should be taken to achieve reliability in the AWS Cloud? (Choose two.)

- A. Use AWS Config to generate an inventory of AWS resources
- B. Use service limits to prevent users from creating or making changes to AWS resources
- C. Use AWS CloudTrail to record AWS API calls into an auditable log file
- D. Use AWS Certificate Manager to whitelist approved AWS resources and services
- E. Use Amazon GuardDuty to validate configuration changes made to AWS resources

Answer(s): A, C

QUESTION: 349

Which service can be used to monitor and receive alerts for AWS account root user AWS Management Console sign-in events?

- A. Amazon CloudWatch
- B. AWS Config
- C. AWS Trusted Advisor
- D. AWS IAM

Answer(s): A

Reference:

<https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity/>

QUESTION: 350

Which design principle should be considered when architecting in the AWS Cloud?

- A. Think of servers as non-disposable resources
- B. Use synchronous integration of services
- C. Design loosely coupled components
- D. Implement the least permissive rules for security groups

Answer(s): C

Reference:

<https://www.botmetric.com/blog/aws-cloud-architecture-design-principles/>

QUESTION: 351

Which AWS services can be used to move data from on-premises data centers to AWS? (Choose two.)

- A. AWS Snowball
- B. AWS Lambda
- C. AWS ElastiCache
- D. AWS Database Migration Service (AWS DMS)
- E. Amazon API Gateway

Answer(s): A, D

Reference:

<https://aws.amazon.com/snowball/>

QUESTION: 352

A batch workload takes 5 hours to finish on an Amazon EC2 instance. The amount of data to be processed doubles monthly and the processing time is proportional.

What is the best cloud architecture to address this consistently growing demand?

- A. Run the application on a bigger EC2 instance size.
- B. Switch to an EC2 instance family that better matches batch requirements.
- C. Distribute the application across multiple EC2 instances and run the workload in parallel.
- D. Run the application on a bare metal EC2 instance.

Answer(s): C

QUESTION: 353

Each department within a company has its own independent AWS account and its own payment method. New company leadership wants to centralize departmental governance and consolidate payments. How can this be achieved using AWS services or features?

- A. Forward monthly invoices for each account. Then create IAM roles to allow cross-account access.
- B. Create a new AWS account. Then configure AWS Organizations and invite all existing accounts to join.
- C. Configure AWS Organizations in each of the existing accounts. Then link all accounts together.
- D. Use Cost Explorer to combine costs from all accounts. Then replicate IAM policies across accounts.

Answer(s): B

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts.html

QUESTION: 354

The ability to horizontally scale Amazon EC2 instances based on demand is an example of which concept in the AWS Cloud value proposition?

- A. Economy of scale
- B. Elasticity
- C. High availability
- D. Agility

Answer(s): B

QUESTION: 355

An ecommerce company anticipates a huge increase in web traffic for two very popular upcoming shopping holidays.

Which AWS service or feature can be configured to dynamically adjust resources to meet this change in demand?

- A. AWS CloudTrail
- B. Amazon EC2 Auto Scaling
- C. Amazon Forecast
- D. AWS Config

Answer(s): B

Reference:

<https://aws.amazon.com/autoscaling/>

QUESTION: 356

Which AWS service enables users to securely connect to AWS resources over the public internet?

- A. Amazon VPC peering
- B. AWS Direct Connect
- C. AWS VPN
- D. Amazon Pinpoint

Answer(s): C

Reference:

[https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf \(36\)](https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf (36))

QUESTION: 357

Which tool is used to forecast AWS spending?

- A. AWS Trusted Advisor
- B. AWS Organizations
- C. Cost Explorer
- D. Amazon Inspector

Answer(s): C

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-forecast.html>

QUESTION: 358

A company is running an ecommerce application hosted in Europe. To decrease latency for users who access the website from other parts of the world, the company would like to cache frequently accessed static content closer to the users.

Which AWS service will support these requirements?

- A. Amazon ElastiCache
- B. Amazon CloudFront
- C. Amazon Elastic File System (Amazon EFS)
- D. Amazon Elastic Block Store (Amazon EBS)

Answer(s): B

Explanation:

Amazon CloudFront employs a global network of edge locations and regional edge caches that cache copies of your content close to your viewers. Amazon CloudFront ensures that end-user requests are served by the closest edge location. As a result, viewer requests travel a short distance, improving performance for your viewers. For files not cached at the edge locations and the regional edge caches, Amazon CloudFront keeps persistent connections with your origin servers so that those files can be fetched from the origin servers as quickly as possible.

Reference:

<https://aws.amazon.com/cloudfront/faqs/>

QUESTION: 359

Which of the following is a component of the AWS Global Infrastructure?

- A. Amazon Alexa
- B. AWS Regions
- C. Amazon Lightsail
- D. AWS Organizations

Answer(s): B

Reference:

<https://aws.amazon.com/about-aws/global-infrastructure/>

QUESTION: 360

Which AWS service will help users determine if an application running on an Amazon EC2 instance has sufficient CPU capacity?

- A. Amazon CloudWatch
- B. AWS Config
- C. AWS CloudTrail
- D. Amazon Inspector

Answer(s): A

Reference:

<https://aws.amazon.com/ec2/faqs/>

QUESTION: 361

Why is it beneficial to use Elastic Load Balancers with applications?

- A. They allow for the conversion from Application Load Balancers to Classic Load Balancers.
- B. They are capable of handling constant changes in network traffic patterns.
- C. They automatically adjust capacity.
- D. They are provided at no charge to users.

Answer(s): B

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html>

QUESTION: 362

Which tasks are the customer's responsibility in the AWS shared responsibility model? (Choose two.)

- A. Infrastructure facilities access management
- B. Cloud infrastructure hardware lifecycle management
- C. Configuration management of user's applications
- D. Networking infrastructure protection
- E. Security groups configuration

Answer(s): C, E

Reference:

<https://cloudacademy.com/blog/aws-shared-responsibility-model-security/>

QUESTION: 363

IT systems should be designed to reduce interdependencies, so that a change or failure in one component does not cascade to other components.

This is an example of which principle of cloud architecture design?

- A. Scalability
- B. Loose coupling
- C. Automation
- D. Automatic scaling

Answer(s): B

Reference:

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf (20)

QUESTION: 364

Which AWS service or feature can enhance network security by blocking requests from a particular network for a web application on AWS? (Choose two.)

- A. AWS WAF
- B. AWS Trusted Advisor
- C. AWS Direct Connect
- D. AWS Organizations
- E. Network ACLs

Answer(s): A, E

Reference:

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

QUESTION: 365

An application runs on multiple Amazon EC2 instances that access a shared file system simultaneously. Which AWS storage service should be used?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon S3
- D. AWS Artifact

Answer(s): B

Reference:

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

QUESTION: 366

A web application is hosted on AWS using an Elastic Load Balancer, multiple Amazon EC2 instances, and Amazon RDS. Which security measures fall under the responsibility of AWS? (Choose two.)

- A. Running a virus scan on EC2 instances
- B. Protecting against IP spoofing and packet sniffing
- C. Installing the latest security patches on the RDS instance
- D. Encrypting communication between the EC2 instances and the Elastic Load Balancer
- E. Configuring a security group and a network access control list (NACL) for EC2

Answer(s): C, D

QUESTION: 367

What is the benefit of elasticity in the AWS Cloud?

- A. Ensure web traffic is automatically spread across multiple AWS Regions.
- B. Minimize storage costs by automatically archiving log data.
- C. Enable AWS to automatically select the most cost-effective services.
- D. Automatically adjust the required compute capacity to maintain consistent performance.

Answer(s): D

Reference:

<https://aimconsulting.com/insights/blog/the-elastic-cloud-opportunity/>

QUESTION: 368

The continual reduction of AWS Cloud pricing is due to:

- A. pay-as-you go pricing
- B. the AWS global infrastructure
- C. economies of scale
- D. reserved storage pricing

Answer(s): C

Reference:

<https://read.acloud.guru/there-are-four-reasons-to-explain-how-using-aws-can-change-the-economic-model-of-the-it-services-850dcc8ea1aa?gi=3bcf6cd0e1e2>

QUESTION: 369

A company needs an Amazon S3 bucket that cannot have any public objects due to compliance requirements. How can this be accomplished?

- A. Enable S3 Block Public Access from the AWS Management Console.
- B. Hold a team meeting to discuss the importance if only uploading private S3 objects.
- C. Require all S3 objects to be manually approved before uploading.
- D. Create a service to monitor all S3 uploads and remove any public uploads.

Answer(s): A

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-block-public-access.html>

QUESTION: 370

A Cloud Practitioner identifies a billing issue after examining the AWS Cost and Usage report in the AWS Management Console. Which action can be taken to resolve this?

- A. Open a detailed case related to billing and submit it to AWS Support for help.
- B. Upload data describing the issue to a new object in a private Amazon S3 bucket.
- C. Create a pricing application and deploy it to a right-sized Amazon EC2 instance for more information.
- D. Proceed with creating a new dashboard in Amazon QuickSight.

Answer(s): A

QUESTION: 371

What does the AWS Simple Monthly Calculator do?

- A. Compares on-premises costs to colocation environments
- B. Estimates monthly billing based on projected usage
- C. Estimates power consumption at existing data centers
- D. Estimates CPU utilization

Answer(s): B

Reference:

<https://aws.amazon.com/blogs/aws/estimate-your-c/>

QUESTION: 372

Who is responsible for patching the guest operating system for Amazon RDS?

- A. The AWS Product team
- B. The customer Database Administrator
- C. Managed partners
- D. AWS Support

Answer(s): A

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 373

Which AWS services may be scaled using AWS Auto Scaling? (Choose two.)

- A. Amazon EC2
- B. Amazon DynamoDB
- C. Amazon S3
- D. Amazon Route 53
- E. Amazon Redshift

Answer(s): A, B

Reference:

<https://aws.amazon.com/autoscaling/faqs/>

QUESTION: 374

Which of the following are benefits of AWS Global Accelerator? (Choose two.)

- A. Reduced cost to run services on AWS
- B. Improved availability of applications deployed on AWS
- C. Higher durability of data stored on AWS
- D. Decreased latency to reach applications deployed on AWS
- E. Higher security of data stored on AWS

Answer(s): B, D

Reference:

<https://aws.amazon.com/global-accelerator/faqs/>

QUESTION: 375

A user who wants to get help with billing and reactivate a suspended account should submit an account and billing request to:

- A. the AWS Support forum
- B. AWS Abuse
- C. an AWS Solutions Architect
- D. AWS Support

Answer(s): D

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/reactivate-suspended-account/>

QUESTION: 376

Which AWS Cloud best practice uses the elasticity and agility of cloud computing?

- A. Provision capacity based on past usage and theoretical peaks
- B. Dynamically and predictively scale to meet usage demands
- C. Build the application and infrastructure in a data center that grants physical access
- D. Break apart the application into loosely coupled components

Answer(s): B

Explanation:

In a traditional computing environment, you provision capacity based on an estimate of a theoretical maximum peak. This can result in periods where expensive resources are sitting idle or occasions of insufficient capacity. With cloud computing, you can access as much or as little capacity as you need and dynamically scale to meet actual demand, while only paying for what you use.

QUESTION: 377

Which method helps to optimize costs of users moving to the AWS Cloud?

- A. Paying only for what is used
- B. Purchasing hardware before it is needed
- C. Manually provisioning cloud resources
- D. Purchasing for the maximum possible load

Answer(s): A

Reference:

<https://www.cloudmanagementinsider.com/ways-to-optimize-aws-cost/>

QUESTION: 378

Under the AWS shared responsibility model, which of the following is a customer responsibility?

- A. Installing security patches for the Xen and KVM hypervisors
- B. Installing operating system patches for Amazon DynamoDB
- C. Installing operating system security patches for Amazon EC2 database instances
- D. Installing operating system security patches for Amazon RDS database instances

Answer(s): C

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 379

The AWS Cost Management tools give users the ability to do which of the following? (Choose two.)

- A. Terminate all AWS resources automatically if budget thresholds are exceeded.
- B. Break down AWS costs by day, service, and linked AWS account.
- C. Create budgets and receive notifications if current or forecasted usage exceeds the budgets.
- D. Switch automatically to Reserved Instances or Spot Instances, whichever is most cost-effective.
- E. Move data stored in Amazon S3 to a more cost-effective storage class.

Answer(s): B, C

QUESTION: 380

Under the AWS shared responsibility model, the security and patching of the guest operating system is the responsibility of:

- A. AWS Support
- B. the customer

- C. AWS Systems Manager
- D. AWS Config

Answer(s): B

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 381

Which AWS service makes it easy to create and manage AWS users and groups, and provide them with secure access to AWS resources at no charge?

- A. AWS Direct Connect
- B. Amazon Connect
- C. AWS Identity and Access Management (IAM)
- D. AWS Firewall Manager

Answer(s): C

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/console_controlling-access.html

<https://aws.amazon.com/iam/>

QUESTION: 381

Which AWS service makes it easy to create and manage AWS users and groups, and provide them with secure access to AWS resources at no charge?

- A. AWS Direct Connect
- B. Amazon Connect
- C. AWS Identity and Access Management (IAM)
- D. AWS Firewall Manager

Answer(s): C

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/console_controlling-access.html

<https://aws.amazon.com/iam/>

QUESTION: 382

Which AWS service provides on-demand of AWS security and compliance documentation?

- A. AWS Directory Service
- B. AWS Artifact
- C. AWS Trusted Advisor
- D. Amazon Inspector

Answer(s): B

Reference:

<https://aws.amazon.com/artifact/#:~:text=AWS%20Artifact%20is%20your%20go,reports%20and%20select%20online%20agreements.>

QUESTION: 383

Which AWS service can be used to turn text into life-like speech?

- A. Amazon Polly
- B. Amazon Transcribe
- C. Amazon Rekognition
- D. Amazon Lex

Answer(s): A**Reference:**

<https://aws.amazon.com/polly/#:~:text=Amazon%20Polly%20is%20a%20service,synthesize%20natural%20sounding%20human%20speech.>

QUESTION: 384

What is one of the core principles to follow when designing a highly available application in the AWS Cloud?

- A. Design using a serverless architecture
- B. Assume that all components within an application can fail
- C. Design AWS Auto Scaling into every application
- D. Design all components using open-source code

Answer(s): B**QUESTION: 385**

A user needs to generate a report that outlines the status of key security checks in an AWS account. The report must include:

- The status of Amazon S3 bucket permissions.
- Whether multi-factor authentication is enabled for the AWS account root user.
- If any security groups are configured to allow unrestricted access.

Where can all this information be found in one location?

- A. Amazon QuickSight dashboard
- B. AWS CloudTrail trails
- C. AWS Trusted Advisor report
- D. IAM credential report

Answer(s): C

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/#Security>

QUESTION: 386

Which Amazon EC2 pricing model should be used to comply with per-core software license requirements?

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

Answer(s): A**Reference:**

<https://aws.amazon.com/ec2/dedicated-hosts/pricing/>

QUESTION: 387

Which of the AWS global infrastructure is used to cache copies of content for faster delivery to users across the globe?

- A. AWS Regions
- B. Availability Zones
- C. Edge locations
- D. Data centers

Answer(s): C**Explanation:**

When your web traffic is geo-dispersed, it's not always feasible and certainly not cost effective to replicate your entire infrastructure across the globe. A CDN provides you the ability to utilize its global network of edge locations to deliver a cached copy of web content such as videos, webpages, images and so on to your customers. To reduce response time, the CDN utilizes the nearest edge location to the customer or originating request location in order to reduce the response time. Throughput is dramatically increased given that the web assets are delivered from cache. For dynamic data, many CDNs can be configured to retrieve data from the origin servers.

Reference:

<https://aws.amazon.com/caching/>

QUESTION: 388

Using AWS Config to record, audit, and evaluate changes to AWS resources to enable traceability is an example of which AWS Well-Architected Framework pillar?

- A. Security

- B. Operational excellence
- C. Performance efficiency
- D. Cost optimization

Answer(s): A

Reference:

https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf (12)

QUESTION: 389

A user needs to quickly deploy a non-relational database on AWS. The user does not want to manage the underlying hardware or the database software.

Which AWS service can be used to accomplish this?

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

Answer(s): B

Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.html>

QUESTION: 390

A Cloud Practitioner is developing a disaster recovery plan and intends to replicate data between multiple geographic areas. Which of the following meets these requirements?

- A. AWS Accounts
- B. AWS Regions
- C. Availability Zones
- D. Edge locations

Answer(s): B

Reference:

<https://www.botmetric.com/blog/having-a-disaster-recovery-plan-is-pivotal-the-dos-and-donts-on-aws-cloud/>

QUESTION: 391

Which features and benefits does the AWS Organizations service provide? (Choose two.)

- A. Establishing real-time communications between members of an internal team
- B. Facilitating the use of NoSQL databases
- C. Providing automated security checks
- D. Implementing consolidated billing

E. Enforcing the governance of AWS accounts

Answer(s): D, E

Reference:

<https://aws.amazon.com/organizations/>

QUESTION: 392

Which AWS service is used to automate configuration management using Chef and Puppet?

- A. AWS Config
- B. AWS OpsWorks
- C. AWS CloudFormation
- D. AWS Systems Manager

Answer(s): B

Reference:

<https://aws.amazon.com/opsworks/>

QUESTION: 393

Which tool is best suited for combining the billing of AWS accounts that were previously independent from one another?

- A. Detailed billing report
- B. Consolidated billing
- C. AWS Cost and Usage report
- D. Cost allocation report

Answer(s): B

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION: 394

The AWS Total Cost of Ownership (TCO) Calculator is used to:

- A. receive reports that break down AWS Cloud compute costs by duration, resource, or tags
- B. estimate savings when comparing the AWS Cloud to an on-premises environment
- C. estimate a monthly bill for the AWS Cloud resources that will be used
- D. enable billing alerts to monitor actual AWS costs compared to estimated costs

Answer(s): B

Reference:

<https://aws.amazon.com/tco-calculator/>

QUESTION: 395

Which AWS services can be used to provide network connectivity between an on-premises network and a VPC? (Choose two.)

- A. Amazon Route 53
- B. AWS Direct Connect
- C. AWS Data Pipeline
- D. AWS VPN
- E. Amazon Connect

Answer(s): B, D

Reference:

<https://aws.amazon.com/directconnect/faqs/>

QUESTION: 396

Under the AWS shared responsibility model, which of the following are customer responsibilities? (Choose two.)

- A. Setting up server-side encryption on an Amazon S3 bucket
- B. Amazon RDS instance patching
- C. Network and firewall configurations
- D. Physical security of data center facilities
- E. Compute capacity availability

Answer(s): A, C

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 397

What is the MINIMUM AWS Support plan level that will provide users with access to the AWS Support API?

- A. Developer
- B. Enterprise
- C. Business
- D. Basic

Answer(s): C

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

QUESTION: 398

A company has deployed several relational databases on Amazon EC2 instances. Every month, the database software vendor releases new security patches that need to be applied to the databases.

What is the MOST efficient way to apply the security patches?

- A. Connect to each database instance on a monthly basis, and download and apply the necessary security patches from the vendor.
- B. Enable automatic patching for the instances using the Amazon RDS console.
- C. In AWS Config, configure a rule for the instances and the required patch level.
- D. Use AWS Systems Manager to automate database patching according to a schedule.

Answer(s): D

Reference:

<https://aws.amazon.com/rds/faqs/>

QUESTION: 399

A company wants to use Amazon Elastic Compute Cloud (Amazon EC2) to deploy a global commercial application. The deployment solution should be built with the highest redundancy and fault tolerance.

Based on this situation, the Amazon EC2 instances should be deployed:

- A. in a single Availability Zone in one AWS Region
- B. with multiple Elastic Network Interfaces belonging to different subnets
- C. across multiple Availability Zones in one AWS Region
- D. across multiple Availability Zones in two AWS Regions

Answer(s): D

Reference:

<https://jayendrapatil.com/aws-high-availability-fault-tolerance-architecture-certification/>

QUESTION: 400

A company has an application with users in both Australia and Brazil. All the company infrastructure is currently provisioned in the Asia Pacific (Sydney) Region in Australia, and Brazilian users are experiencing high latency. What should the company do to reduce latency?

- A. Implement AWS Direct Connect for users in Brazil
- B. Provision resources in the South America (São Paulo) Region in Brazil
- C. Use AWS Transit Gateway to quickly route users from Brazil to the application
- D. Launch additional Amazon EC2 instances in Sydney to handle the demand

Answer(s): B

Reference:

<https://aws.amazon.com/transit-gateway/>

QUESTION: 401

An Amazon EC2 instance runs only when needed yet must remain active for the duration of the process. What is the most appropriate purchasing option?

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

Answer(s): C**Reference:**

<https://jayendrapatil.com/aws-ec2-instance-purchasing-option/>

QUESTION: 402

Which AWS dashboard displays relevant and timely information to help users manage events in progress, and provides proactive notifications to help plan for scheduled activities?

- A. AWS Service Health Dashboard
- B. AWS Personal Health Dashboard
- C. AWS Trusted Advisor dashboard
- D. Amazon CloudWatch dashboard

Answer(s): B**Reference:**

<https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/>

QUESTION: 403

Which AWS hybrid storage service enables a user's on-premises applications to seamlessly use AWS Cloud storage?

- A. AWS Backup
- B. Amazon Connect
- C. AWS Direct Connect
- D. AWS Storage Gateway

Answer(s): D**Reference:**

<https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

QUESTION: 404

Which of the following acts as a virtual firewall at the Amazon EC2 instance level to control traffic for one or more instances?

- A. Access keys
- B. Virtual private gateways
- C. Security groups
- D. Access Control Lists (ACL)

Answer(s): C

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html>

QUESTION: 405

What is the most efficient way to establish network connectivity from on-premises to multiple VPCs in different AWS Regions?

- A. Use AWS Direct Connect
- B. Use AWS VPN
- C. Use AWS Client VPN
- D. Use an AWS Transit Gateway

Answer(s): D

Reference:

<https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf> (11)

QUESTION: 406

Which AWS Support plan provides access to architectural and operational reviews, as well as 24/7 access to Senior Cloud Support Engineers through email, online chat, and phone?

- A. Basic
- B. Business
- C. Developer
- D. Enterprise

Answer(s): D

Reference:

<https://aws.amazon.com/premiumsupport/plans/enterprise/>

QUESTION: 407

Which AWS service or feature helps restrict the AWS services, resources, and individual API actions the users and roles in each member account can access?

- A. Amazon Cognito
- B. AWS Organizations
- C. AWS Shield

D. AWS Firewall Manager

Answer(s): B

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html

QUESTION: 408

What is the best resource for a user to find compliance-related information and reports about AWS?

- A. AWS Artifact
- B. AWS Marketplace
- C. Amazon Inspector
- D. AWS Support

Answer(s): A

Reference:

<https://aws.amazon.com/compliance/faq/>

QUESTION: 409

Which Amazon S3 storage class is optimized to provide access to data with lower resiliency requirements, but rapid access when needed such as duplicate backups?

- A. Amazon S3 Standard
- B. Amazon S3 Glacier Deep Archive
- C. Amazon S3 One Zone-Infrequent Access
- D. Amazon S3 Glacier

Answer(s): C

Reference:

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

QUESTION: 410

What is an Availability Zone in AWS?

- A. One or more physical data centers
- B. A completely isolated geographic location
- C. One or more edge locations based around the world
- D. A data center location with a single source of power and networking

Answer(s): A

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

QUESTION: 411

Which AWS services can be used as infrastructure automation tools? (Choose two.)

- A. AWS CloudFormation
- B. Amazon CloudFront
- C. AWS Batch
- D. AWS OpsWorks
- E. Amazon QuickSight

Answer(s): A, D

Reference:

<https://blog.newrelic.com/engineering/best-cloud-infrastructure-automation-tools/>

QUESTION: 412

Which AWS service enables users to create copies of resources across AWS Regions?

- A. Amazon ElastiCache
- B. AWS CloudFormation
- C. AWS CloudTrail
- D. AWS Systems Manager

Answer(s): B

Reference:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html>

QUESTION: 413

A user would like to encrypt data that is received, stored, and managed by AWS CloudTrail.

Which AWS service will provide this capability?

- A. AWS Secrets Manager
- B. AWS Systems Manager
- C. AWS Key Management Service (AWS KMS)
- D. AWS Certificate Manager

Answer(s): C

Reference:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/data-protection.html>

QUESTION: 414

Which AWS Cloud benefit eliminates the need for users to try estimating future infrastructure usage?

- A. Easy and fast deployment of applications in multiple Regions around the world
- B. Security of the AWS Cloud

- C. Elasticity of the AWS Cloud
- D. Lower variable costs due to massive economies of scale

Answer(s): C

QUESTION: 415

What credential components are required to gain programmatic access to an AWS account?
(Choose two.)

- A. An access key ID
- B. A primary key
- C. A secret access key
- D. A user ID
- E. A secondary key

Answer(s): A, C

Reference:

<https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

QUESTION: 416

Which of the following are AWS compute services? (Select two.)

- A. Amazon Lightsail
- B. AWS Systems Manager
- C. AWS CloudFormation
- D. AWS Batch
- E. Amazon Inspector

Answer(s): A, D

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/compute-services.html>

QUESTION: 417

How can a company separate costs for network traffic, Amazon EC2, Amazon S3, and other AWS services by department?

- A. Add department-specific tags to each resource
- B. Create a separate VPC for each department
- C. Create a separate AWS account for each department
- D. Use AWS Organizations

Answer(s): A

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html#allocation-how>

QUESTION: 418

What is a benefit of consolidated billing for AWS accounts?

- A. Access to AWS Personal Health Dashboard
- B. Combined usage volume discounts
- C. Improved account security
- D. Centralized AWS IAM

Answer(s): B

Reference:

<https://jayendrapatil.com/aws-consolidated-billing/>

QUESTION: 419

Which AWS service will allow a user to set custom cost and usage limits, and will alert when the thresholds are exceeded?

- A. AWS Organizations
- B. AWS Budgets
- C. Cost Explorer
- D. AWS Trusted Advisor

Answer(s): B

Reference:

<https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/>

QUESTION: 420

Which AWS service provides the ability to detect inadvertent data leaks of personally identifiable information (PII) and user credential data?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. Amazon Macie
- D. AWS Shield

Answer(s): C

Reference:

<https://aws.amazon.com/macie/>

QUESTION: 421

Which tool can be used to monitor AWS service limits?

- A. AWS Total Cost of Ownership (TCO) Calculator
- B. AWS Trusted Advisor
- C. AWS Personal Health Dashboard
- D. AWS Cost and Usage report

Answer(s): B

Reference:

<https://aws.amazon.com/blogs/mt/monitoring-service-limits-with-trusted-advisor-and-amazon-cloudwatch/>

QUESTION: 422

A company has distributed its workload on both the AWS Cloud and some on-premises servers. What type of architecture is this?

- A. Virtual private network
- B. Virtual private cloud
- C. Hybrid cloud
- D. Private cloud

Answer(s): C

Reference:

<https://aws.amazon.com/hybrid/>

QUESTION: 423

Which of the following describes a security best practice that can be implemented using AWS IAM?

- A. Disable AWS Management Console access for all users
- B. Generate secret keys for every IAM user
- C. Grant permissions to users who are required to perform a given task only
- D. Store AWS credentials within Amazon EC2 instances

Answer(s): C

Reference:

<https://cloudcheckr.com/cloud-security/top-5-iam-best-practices/>

QUESTION: 424

What can be used to automate and manage secure, well-architected, multi-account AWS environments?

- A. AWS shared responsibility model
- B. AWS Control Tower
- C. AWS Security Hub

D. AWS Well-Architected Tool

Answer(s): B

Explanation:

Control Tower automates the process of setting up a new baseline multi-account AWS environment that is secure, well-architected, and ready to use. Control Tower incorporates the knowledge that AWS Professional Service has gained over the course of thousands of successful customer engagements.

Reference:

<https://aws.amazon.com/blogs/aws/aws-control-tower-set-up-govern-a-multi-account-aws-environment/>

QUESTION: 425

Which AWS service or feature allows a user to easily scale connectivity among thousands of VPCs?

- A. VPC peering
- B. AWS Transit Gateway
- C. AWS Direct Connect
- D. AWS Global Accelerator

Answer(s): B

Reference:

<https://aws.amazon.com/blogs/training-and-certification/explore-the-aws-transit-gateway-networking-and-scaling-digital-course/>

QUESTION: 426

A company needs protection from expanded distributed denial of service (DDoS) attacks on its website and assistance from AWS experts during such events.

Which AWS managed service will meet these requirements?

- A. AWS Shield Advanced
- B. AWS Firewall Manager
- C. AWS WAF
- D. Amazon GuardDuty

Answer(s): A

Reference:

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html>

QUESTION: 427

A company's application has flexible start and end times.

Which Amazon EC2 pricing model will be the MOST cost-effective?

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

Answer(s): B

Reference:

<https://aws.amazon.com/ec2/pricing/>

QUESTION: 428

Under the AWS shared responsibility model, what are the customer's responsibilities? (Choose two.)

- A. Physical and environmental security
- B. Physical network devices including firewalls
- C. Storage device decommissioning
- D. Security of data in transit
- E. Data integrity authentication

Answer(s): D, E

QUESTION: 429

A cloud practitioner has a data analysis workload that is infrequently executed and can be interrupted without harm. To optimize for cost, which Amazon EC2 purchasing option should be used?

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

Answer(s): C

Reference:

<https://aws.amazon.com/ec2/pricing/>

QUESTION: 430

Which AWS container service will help a user install, operate, and scale the cluster management infrastructure?

- A. Amazon Elastic Container Registry (Amazon ECR)
- B. AWS Elastic Beanstalk
- C. Amazon Elastic Container Service (Amazon ECS)
- D. Amazon Elastic Block Store (Amazon EBS)

Answer(s): C

QUESTION: 431

Which of the following allows an application running on an Amazon EC2 instance to securely write data to an Amazon S3 bucket without using long term credentials?

- A. Amazon Cognito
- B. AWS Shield
- C. AWS IAM role
- D. AWS IAM user access key

Answer(s): C

QUESTION: 432

A company with a Developer-level AWS Support plan provisioned an Amazon RDS database and cannot connect to it. Who should the developer contact for this level of support?

- A. AWS Support using a support case
- B. AWS Professional Services
- C. AWS technical account manager
- D. AWS consulting partners

Answer(s): A

QUESTION: 433

What is the purpose of having an internet gateway within a VPC?

- A. To create a VPN connection to the VPC
- B. To allow communication between the VPC and the Internet
- C. To impose bandwidth constraints on internet traffic
- D. To load balance traffic from the Internet across Amazon EC2 instances

Answer(s): B

QUESTION: 434

A company must ensure that its endpoint for a database instance remains the same after a single Availability Zone service interruption. The application needs to resume database operations without the need for manual administrative intervention. How can these requirements be met?

- A. Use multiple Amazon Route 53 routes to the standby database instance endpoint hosted on AWS Storage Gateway.

- B. Configure Amazon RDS Multi-Availability Zone deployments with automatic failover to the standby
- C. Add multiple Application Load Balancers and deploy the database instance with AWS Elastic Beanstalk.
- D. Deploy a single Network Load Balancer to distribute incoming traffic across multiple Amazon CloudFront origins.

Answer(s): B

QUESTION: 435

Which AWS managed service can be used to distribute traffic between one or more Amazon EC2 instances?

- A. NAT gateway
- B. Elastic Load Balancing
- C. Amazon Athena
- D. AWS PrivateLink

Answer(s): B

QUESTION: 436

AWS Trusted Advisor provides recommendations on which of the following? (Choose two.)

- A. Cost optimization
- B. Auditing
- C. Serverless architecture
- D. Performance
- E. Scalability

Answer(s): A, D

QUESTION: 437

Which of the following tasks can only be performed after signing in with AWS account root user credentials? (Choose two.)

- A. Closing an AWS account
- B. Creating a new IAM policy
- C. Changing AWS Support plans
- D. Attaching a role to an Amazon EC2 instance
- E. Generating access keys for IAM users

Answer(s): A, C

QUESTION: 438

Fault tolerance refers to:

- A. the ability of an application to accommodate growth without changing design
- B. how well and how quickly an application's environment can have lost data restored
- C. how secure your application is
- D. the built-in redundancy of an application's components

Answer(s): B

QUESTION: 439

A company operating in the AWS Cloud requires separate invoices for specific environments, such as development, testing, and production. How can this be achieved?

- A. Use multiple AWS accounts
- B. Use resource tagging
- C. Use multiple VPCs
- D. Use Cost Explorer

Answer(s): B

QUESTION: 440

Which AWS service can be used in the application deployment process?

- A. AWS AppSync
- B. AWS Batch
- C. AWS CodePipeline
- D. AWS DataSync

Answer(s): C

QUESTION: 441

What can be used to reduce the cost of running Amazon EC2 instances? (Choose two.)

- A. Spot Instances for stateless and flexible workloads
- B. Memory optimized instances for high-compute workloads
- C. On-Demand Instances for high-cost and sustained workloads
- D. Reserved Instances for sustained workloads
- E. Spend limits set using AWS Budgets

Answer(s): A, D

QUESTION: 442

A company is launching an e-commerce site that will store and process credit card data. The company requires information about AWS compliance reports and AWS agreements. Which AWS service provides on-demand access to these items?

- A. AWS Certificate Manager
- B. AWS Config
- C. AWS Artifact
- D. AWS CloudTrail

Answer(s): C

QUESTION: 443

Which AWS service or feature allows the user to manage cross-region application traffic?

- A. Amazon AppStream 2.0
- B. Amazon VPC
- C. Elastic Load Balancer
- D. Amazon Route 53

Answer(s): A

QUESTION: 444

Which AWS service can be used to track unauthorized API calls?

- A. AWS Config
- B. AWS CloudTrail
- C. AWS Trusted Advisor
- D. Amazon Inspector

Answer(s): B

QUESTION: 445

A user needs to regularly audit and evaluate the setup of all AWS resources, identify non-compliant accounts, and be notified when a resource changes.

Which AWS service can be used to meet these requirements?

- A. AWS Trusted Advisor
- B. AWS Config
- C. AWS Resource Access Manager
- D. AWS Systems Manager

Answer(s): B

QUESTION: 446

A user is planning to launch two additional Amazon EC2 instances to increase availability. Which action should the user take?

- A. Launch the instances across multiple Availability Zones in a single AWS Region.
- B. Launch the instances as EC2 Reserved Instances in the same AWS Region and the same Availability Zone.
- C. Launch the instances in multiple AWS Regions, but in the same Availability Zone.
- D. Launch the instances as EC2 Spot Instances in the same AWS Region, but in different Availability Zones.

Answer(s): A

QUESTION: 447

A company must store critical business data in Amazon S3 with a backup to another AWS Region. How can this be achieved?

- A. Use an Amazon CloudFront Content Delivery Network (CDN) to cache data globally
- B. Set up Amazon S3 cross-region replication to another AWS Region
- C. Configure the AWS Backup service to back up to the data to another AWS Region
- D. Take Amazon S3 bucket snapshots and copy that data to another AWS Region

Answer(s): B

QUESTION: 448

Which AWS Cloud service can send alerts to customers if custom spending thresholds are exceeded?

- A. AWS Budgets
- B. AWS Cost Explorer
- C. AWS Cost Allocation Tags
- D. AWS Organizations

Answer(s): A

QUESTION: 449

What is the recommended method to request penetration testing on AWS resources?

- A. Open a support case
- B. Fill out the Penetration Testing Request Form
- C. Request a penetration test from your technical account manager
- D. Contact your AWS sales representative

Answer(s): B

QUESTION: 450

A user needs to automatically discover, classify, and protect sensitive data stored in Amazon S3. Which AWS service can meet these requirements?

- A. Amazon Inspector
- B. Amazon Macie
- C. Amazon GuardDuty
- D. AWS Secrets Manager

Answer(s): B

QUESTION: 451

Which components are required to build a successful site-to-site VPN connection on AWS? (Choose two.)

- A. Internet gateway
- B. NAT gateway
- C. Customer gateway
- D. Transit gateway
- E. Virtual private gateway

Answer(s): C, D

QUESTION: 452

Which Amazon EC2 pricing option is best suited for applications with short-term, spiky, or unpredictable workloads that cannot be interrupted?

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

Answer(s): C

QUESTION: 453

Which AWS cloud architecture principle states that systems should reduce interdependencies?

- A. Scalability
- B. Services, not servers
- C. Removing single points of failure
- D. Loose coupling

Answer(s): D

QUESTION: 454

What is the MOST effective resource for staying up to date on AWS security announcements?

- A. AWS Personal Health Dashboard
- B. AWS Secrets Manager
- C. AWS Security Bulletins
- D. Amazon Inspector

Answer(s): C

QUESTION: 455

Which AWS service offers persistent storage for a file system?

- A. Amazon S3
- B. Amazon EC2 instance store
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon ElastiCache

Answer(s): C

QUESTION: 456

Which of the following allows AWS users to manage cost allocations for billing?

- A. Tagging resources
- B. Limiting who can create resources
- C. Adding a secondary payment method
- D. Running all operations on a single AWS account

Answer(s): A

QUESTION: 457

Which AWS service allows users to download security and compliance reports about the AWS infrastructure on demand?

- A. Amazon GuardDuty
- B. AWS Security Hub
- C. AWS Artifact
- D. AWS Shield

Answer(s): C

QUESTION: 458

Which of the following AWS services are serverless? (Choose two.)

- A. AWS Lambda
- B. Amazon Elasticsearch Service
- C. AWS Elastic Beanstalk
- D. Amazon DynamoDB
- E. Amazon Redshift

Answer(s): A, D

QUESTION: 459

Which AWS managed services can be used to extend an on-premises data center to the AWS network? (Choose two.)

- A. AWS VPN
- B. NAT gateway
- C. AWS Direct Connect
- D. Amazon Connect
- E. Amazon Route 53

Answer(s): A, C

QUESTION: 460

Which requirement must be met for a member account to be unlinked from an AWS Organizations account?

- A. The linked account must be actively compliant with AWS System and Organization Controls (SOC).
- B. The payer and the linked account must both create AWS Support cases to request that the member account be unlinked from the organization.
- C. The member account must meet the requirements of a standalone account.
- D. The payer account must be used to remove the linked account from the organization.

Answer(s): D

QUESTION: 461

What AWS benefit refers to a customer's ability to deploy applications that scale up and down to meet variable demand?

- A. Elasticity
- B. Agility
- C. Security
- D. Scalability

Answer(s): D

QUESTION: 462

During a compliance review, one of the auditors requires a copy of the AWS SOC 2 report. Which service should be used to submit this request?

- A. AWS Personal Health Dashboard
- B. AWS Trusted Advisor
- C. AWS Artifact
- D. Amazon S3

Answer(s): C

QUESTION: 463

A company wants to set up a highly available workload in AWS with a disaster recovery plan that will allow the company to recover in case of a regional service interruption.

Which configuration will meet these requirements?

- A. Run on two Availability Zones in one AWS Region, using the additional Availability Zones in the AWS Region for the disaster recovery site.
- B. Run on two Availability Zones in one AWS Region, using another AWS Region for the disaster recovery site.
- C. Run on two Availability Zones in one AWS Region, using a local AWS Region for the disaster recovery site.
- D. Run across two AWS Regions, using a third AWS Region for the disaster recovery site.

Answer(s): A

Reference:

<https://aws.amazon.com/blogs/startups/large-scale-disaster-recovery-using-aws-regions/>

QUESTION: 464

A company has a 500 TB image repository that needs to be transported to AWS for processing. Which AWS service can import this data MOST cost-effectively?

- A. AWS Snowball
- B. AWS Direct Connect
- C. AWS VPN
- D. Amazon S3

Answer(s): D

Reference:

<https://aws.amazon.com/blogs/storage/migrating-hundreds-of-tb-of-data-to-amazon-s3-with-aws-datasync/>

QUESTION: 465

Which AWS service can run a managed PostgreSQL database that provides online transaction processing (OLTP)?

- A. Amazon DynamoDB
- B. Amazon Athena
- C. Amazon RDS
- D. Amazon EMR

Answer(s): C**Reference:**

<https://aws.amazon.com/rds/postgresql/>

QUESTION: 466

Which of the following assist in identifying costs by department? (Choose two.)

- A. Using tags on resources
- B. Using multiple AWS accounts
- C. Using an account manager
- D. Using AWS Trusted Advisor
- E. Using Consolidated Billing

Answer(s): B, E**QUESTION: 467**

A company wants to allow full access to an Amazon S3 bucket for a particular user.

Which element in the S3 bucket policy holds the user details that describe who needs access to the S3 bucket?

- A. Principal
- B. Action
- C. Resource
- D. Statement

Answer(s): C**Reference:**

<https://docs.aws.amazon.com/AmazonS3/latest/dev/walkthrough1.html>

QUESTION: 468

Which AWS service allows for effective cost management of multiple AWS accounts?

- A. AWS Organizations
- B. AWS Trusted Advisor
- C. AWS Direct Connect

D. Amazon Connect

Answer(s): A

Reference:

<https://aws.amazon.com/blogs/aws/aws-organizations-policy-based-management-for-multiple-aws-accounts/>

QUESTION: 469

A company is piloting a new customer-facing application on Amazon Elastic Compute Cloud (Amazon EC2) for one month. What pricing model is appropriate?

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

Answer(s): C

Reference:

<https://aws.amazon.com/ec2/pricing/>

QUESTION: 470

Which AWS tools automatically forecast future AWS costs?

- A. AWS Support Center
- B. AWS Total Cost of Ownership (TCO) Calculator
- C. AWS Simple Monthly Calculator
- D. Cost Explorer

Answer(s): D

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-forecast.html>

QUESTION: 471

Under the AWS shared responsibility model, which of the following is a responsibility of AWS?

- A. Enabling server-side encryption for objects stored in S3
- B. Applying AWS IAM security policies
- C. Patching the operating system on an Amazon EC2 instance
- D. Applying updates to the hypervisor

Answer(s): D

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/?ref=wellarchitected>

QUESTION: 472

A user is able to set up a master payer account to view consolidated billing reports through:

- A. AWS Budgets.
- B. Amazon Macie.
- C. Amazon QuickSight.
- D. AWS Organizations.

Answer(s): D**Reference:**

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION: 473

Performing operations as code is a design principle that supports which pillar of the AWS Well-Architected Framework?

- A. Performance efficiency
- B. Operational excellence
- C. Reliability
- D. Security

Answer(s): B**Reference:**

<https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/>

QUESTION: 474

Which design principle is achieved by following the reliability pillar of the AWS Well-Architected Framework?

- A. Vertical scaling
- B. Manual failure recovery
- C. Testing recovery procedures
- D. Changing infrastructure manually

Answer(s): C**Reference:**

<https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/>

QUESTION: 475

What is a characteristic of Convertible Reserved Instances (RIs)?

- A. Users can exchange Convertible RIs for other Convertible RIs from a different instance family.

- B. Users can exchange Convertible RIs for other Convertible RIs in different AWS Regions.
- C. Users can sell and buy Convertible RIs on the AWS Marketplace.
- D. Users can shorten the term of their Convertible RIs by merging them with other Convertible RIs.

Answer(s): A

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-convertible-exchange.html>

QUESTION: 476

The user is fully responsible for which action when running workloads on AWS?

- A. Patching the infrastructure components
- B. Implementing controls to route application traffic
- C. Maintaining physical and environmental controls
- D. Maintaining the underlying infrastructure components

Answer(s): B

QUESTION: 477

An architecture design includes Amazon EC2, an Elastic Load Balancer, and Amazon RDS. What is the BEST way to get a monthly cost estimation for this architecture?

- A. Open an AWS Support case, provide the architecture proposal, and ask for a monthly cost estimation.
- B. Collect the published prices of the AWS services and calculate the monthly estimate.
- C. Use the AWS Simple Monthly Calculator to estimate the monthly cost.
- D. Use the AWS Total Cost of Ownership (TCO) Calculator to estimate the monthly cost.

Answer(s): C

Reference:

<https://docs.aws.amazon.com/pricing-calculator/latest/userguide/aws-pc.pdf>

QUESTION: 478

Which are benefits of using Amazon RDS over Amazon EC2 when running relational databases on AWS? (Choose two.)

- A. Automated backups
- B. Schema management
- C. Indexing of tables
- D. Software patching
- E. Extract, transform, and load (ETL) management

Answer(s): A, D

Reference:

[**QUESTION: 479**](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide>Welcome.html</p></div><div data-bbox=)

What does the Amazon S3 Intelligent-Tiering storage class offer?

- A. Payment flexibility by reserving storage capacity
- B. Long-term retention of data by copying the data to an encrypted Amazon Elastic Block Store (Amazon EBS) volume
- C. Automatic cost savings by moving objects between tiers based on access pattern changes
- D. Secure, durable, and lowest cost storage for data archival

Answer(s): C**Reference:**

<https://aws.amazon.com/about-aws/whats-new/2018/11/s3-intelligent-tiering/>

QUESTION: 480

A company has multiple data sources across the organization and wants to consolidate data into one data warehouse. Which AWS service can be used to meet this requirement?

- A. Amazon DynamoDB
- B. Amazon Redshift
- C. Amazon Athena
- D. Amazon QuickSight

Answer(s): B**Reference:**

<https://aws.amazon.com/redshift/faqs/>

QUESTION: 481

Which AWS service can be used to track resource changes and establish compliance?

- A. Amazon CloudWatch
- B. AWS Config
- C. AWS CloudTrail
- D. AWS Trusted Advisor

Answer(s): B**Reference:**

<https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html>

QUESTION: 482

A user has underutilized on-premises resources.

Which AWS Cloud concept can BEST address this issue?

- A. High availability
- B. Elasticity
- C. Security
- D. Loose coupling

Answer(s): B

Reference:

<https://www.gremlin.com/blog/implementing-cost-saving-strategies-on-amazon-ec-2-with-chaos-engineering/>

QUESTION: 483

A user has a stateful workload that will run on Amazon EC2 for the next 3 years. What is the MOST cost-effective pricing model for this workload?

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

Answer(s): A

Explanation:

On-demand instances are useful for running stateful workloads without making a long-term commitment, but if your workloads are stateless or can tolerate shorter run cycles, there's a more cost-effective instance type called a Spot Instance.

Reference:

<https://www.gremlin.com/blog/implementing-cost-saving-strategies-on-amazon-ec-2-with-chaos-engineering/>

QUESTION: 484

A cloud practitioner needs an Amazon EC2 instance to launch and run for 7 hours without interruptions. What is the most suitable and cost-effective option for this task?

- A. On-Demand Instance
- B. Reserved Instance
- C. Dedicated Host
- D. Spot Instance

Answer(s): D

Reference:

<https://aws.amazon.com/ec2/spot/details/>

QUESTION: 485

Which of the following are benefits of using AWS Trusted Advisor? (Choose two.)

- A. Providing high-performance container orchestration
- B. Creating and rotating encryption keys
- C. Detecting underutilized resources to save costs
- D. Improving security by proactively monitoring the AWS environment
- E. Implementing enforced tagging across AWS resources

Answer(s): D, E

Reference:

<https://aws.amazon.com/about-aws/whats-new/2016/06/aws-support-enables-tagging-capabilities-for-trusted-advisor/>

QUESTION: 486

A developer has been hired by a large company and needs AWS credentials.

Which are security best practices that should be followed? (Choose two.)

- A. Grant the developer access to only the AWS resources needed to perform the job.
- B. Share the AWS account root user credentials with the developer.
- C. Add the developer to the administrator's group in AWS IAM.
- D. Configure a password policy that ensures the developer's password cannot be changed.
- E. Ensure the account password policy requires a minimum length.

Answer(s): A, E

QUESTION: 487

Which AWS storage service is designed to transfer petabytes of data in and out of the cloud?

- A. AWS Storage Gateway
- B. Amazon S3 Glacier Deep Archive
- C. Amazon Lightsail
- D. AWS Snowball

Answer(s): D

Reference:

<https://docs.aws.amazon.com/snowball/latest/ug/transfer-petabytes.html>

QUESTION: 488

Which service provides a user the ability to warehouse data in the AWS Cloud?

- A. Amazon EFS
- B. Amazon Redshift
- C. Amazon RDS
- D. Amazon VPC

Answer(s): B

Reference:

<https://aws.amazon.com/redshift/>

QUESTION: 489

A user is planning to migrate an application workload to the AWS Cloud.

Which control becomes the responsibility of AWS once the migration is complete?

- A. Patching the guest operating system
- B. Maintaining physical and environmental controls
- C. Protecting communications and maintaining zone security
- D. Patching specific applications

Answer(s): B

QUESTION: 490

Which services can be used to deploy applications on AWS? (Choose two.)

- A. AWS Elastic Beanstalk
- B. AWS Config
- C. AWS OpsWorks
- D. AWS Application Discovery Service
- E. Amazon Kinesis

Answer(s): A, C

Reference:

<https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-on-aws.pdf>

QUESTION: 491

Which AWS service can be used to provide an on-demand, cloud-based contact center?

- A. AWS Direct Connect
- B. Amazon Connect
- C. AWS Support Center
- D. AWS Managed Services

Answer(s): B

Reference:

<https://aws.amazon.com/connect/customers/>

QUESTION: 492

What tool enables customers without an AWS account to estimate costs for almost all AWS services?

- A. Cost Explorer
- B. TCO Calculator
- C. AWS Budgets
- D. Simple Monthly Calculator

Answer(s): A

Reference:

<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>

QUESTION: 493

Which component must be attached to a VPC to enable inbound Internet access?

- A. NAT gateway
- B. VPC endpoint
- C. VPN connection
- D. Internet gateway

Answer(s): C

Reference:

<https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf> (41, 42, 43)

QUESTION: 494

Which pricing model would result in maximum Amazon Elastic Compute Cloud (Amazon EC2) savings for a database server that must be online for one year?

- A. Spot Instance
- B. On-Demand Instance
- C. Partial Upfront Reserved Instance
- D. No Upfront Reserved Instance

Answer(s): C

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html>

QUESTION: 495

A company has a MySQL database running on a single Amazon EC2 instance. The company now requires higher availability in the event of an outage. Which set of tasks would meet this requirement?

- A. Add an Application Load Balancer in front of the EC2 instance
- B. Configure EC2 Auto Recovery to move the instance to another Availability Zone
- C. Migrate to Amazon RDS and enable Multi-AZ
- D. Enable termination protection for the EC2 instance to avoid outages

Answer(s): C

Reference:

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

QUESTION: 496

A company wants to ensure that AWS Management Console users are meeting password complexity requirements. How can the company configure password complexity?

- A. Using an AWS IAM user policy
- B. Using an AWS Organizations service control policy (SCP)
- C. Using an AWS IAM account password policy
- D. Using an AWS Security Hub managed insight

Answer(s): A

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

QUESTION: 497

Under the AWS shared responsibility model, which of the following is the customer's responsibility?

- A. Patching guest OS and applications
- B. Patching and fixing flaws in the infrastructure
- C. Physical and environmental controls
- D. Configuration of AWS infrastructure devices

Answer(s): A

QUESTION: 498

Which of the following tasks is required to deploy a PCI-compliant workload on AWS?

- A. Use any AWS service and implement PCI controls at the application layer
- B. Use an AWS service that is in-scope for PCI compliance and raise an AWS support ticket to enable PCI compliance at the application layer
- C. Use any AWS service and raise an AWS support ticket to enable PCI compliance on that service
- D. Use an AWS service that is in scope for PCI compliance and apply PCI controls at the application layer

Answer(s): D

Reference:

<https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-pci-controls.html>

QUESTION: 499

A company is building an application that requires the ability to send, store, and receive messages between application components. The company has another requirement to process messages in first-in, first-out (FIFO) order.

Which AWS service should the company use?

- A. AWS Step Functions
- B. Amazon Simple Notification Service (Amazon SNS)
- C. Amazon Kinesis Data Streams
- D. Amazon Simple Queue Service (Amazon SQS)

Answer(s): D

Reference:

<https://aws.amazon.com/sqs/faqs/>

QUESTION: 500

AnyCompany recently purchased Example Corp. Both companies use AWS resources, and AnyCompany wants a single aggregated bill.

Which option allows AnyCompany to receive a single bill?

- A. Example Corp. must submit a request to its AWS solutions architect or AWS technical account manager to link the accounts and consolidate billing.
- B. AnyCompany must create a new support case in the AWS Support Center requesting that both bills be combined.
- C. Send an invitation to join the organization from AnyCompany's AWS Organizations master account to Example Corp.
- D. Migrate the Example Corp. VPCs, Amazon EC2 instances, and other resources into the AnyCompany AWS account.

Answer(s): D

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf>

QUESTION: 501

Which tool can be used to create alerts when the actual or forecasted cost of AWS services exceeds a certain threshold?

- A. Cost Explorer
- B. AWS Budgets
- C. AWS Cost and Usage Report
- D. AWS CloudTrail

Answer(s): B

Reference:

<https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/>

QUESTION: 502

A user has limited knowledge of AWS services, but wants to quickly deploy a scalable Node.js application in the AWS Cloud. Which service should be used to deploy the application?

- A. AWS CloudFormation
- B. AWS Elastic Beanstalk
- C. Amazon EC2
- D. AWS OpsWorks

Answer(s): B

Reference:

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

QUESTION: 503

Which AWS Trusted Advisor check is available to all AWS users?

- A. Core checks
- B. All checks
- C. Cost optimization checks
- D. Fault tolerance checks

Answer(s): C

Reference:

<https://www.amazonaws.cn/en/support/trustedadvisor/faq/#checks>

QUESTION: 504

A web developer is concerned that a DDoS attack could target an application.

Which AWS services or features can help protect against such an attack? (Choose two.)

- A. AWS Shield
- B. AWS CloudTrail
- C. Amazon CloudFront
- D. AWS Support Center
- E. AWS Service Health Dashboard

Answer(s): A, B

Reference:

<https://aws.amazon.com/shield/>

QUESTION: 505

Which AWS service gives users on-demand, self-service access to AWS compliance control reports?

- A. AWS Config
- B. Amazon GuardDuty
- C. AWS Trusted Advisor
- D. AWS Artifact

Answer(s): D

Reference:

<https://aws.amazon.com/artifact>

QUESTION: 506

A company wants to provide one of its employees with access to Amazon RDS. The company also wants to limit the interaction to only the AWS CLI and AWS software development kits (SDKs).

Which combination of actions should the company take to meet these requirements while following the principles of least privilege? (Choose two.)

- A. Create an IAM user and provide AWS Management Console access only.
- B. Create an IAM user and provide programmatic access only.
- C. Create an IAM role and provide AWS Management Console access only.
- D. Create an IAM policy with administrator access and attach it to the IAM user.
- E. Create an IAM policy with Amazon RDS access and attach it to the IAM user.

Answer(s): B, E

QUESTION: 507

A company has a compliance requirement to record and evaluate configuration changes, as well as perform remediation actions on AWS resources.

Which AWS service should the company use?

- A. AWS Config
- B. AWS Secrets Manager
- C. AWS CloudTrail
- D. AWS Trusted Advisor

Answer(s): A

Reference:

<https://aws.amazon.com/config/>

QUESTION: 508

What are the advantages of deploying an application with Amazon EC2 instances in multiple Availability Zones? (Choose two.)

- A. Preventing a single point of failure
- B. Reducing the operational costs of the application
- C. Allowing the application to serve cross-region users with low latency
- D. Increasing the availability of the application
- E. Increasing the load of the application

Answer(s): A, D**Reference:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>

QUESTION: 509

A workload on AWS will run for the foreseeable future by using a consistent number of Amazon EC2 instances. What pricing model will minimize cost while ensuring that compute resources remain available?

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

Answer(s): D**Reference:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html>

QUESTION: 510

Which tool can be used to identify scheduled changes to the AWS infrastructure?

- A. AWS Personal Health Dashboard
- B. AWS Trusted Advisor
- C. Billing Dashboard
- D. AWS Config

Answer(s): A**Reference:**

<https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/>

QUESTION: 511

Which of the following is the customer's responsibility when using Amazon RDS?

- A. Patching the operating system of underlying hardware

- B. Controlling traffic to and from the database through security groups
- C. Running backups that enable point-in-time recovery of a DB instance
- D. Replacing failed DB instances

Answer(s): D

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.html>

QUESTION: 512

What is the customer's responsibility when using AWS Lambda?

- A. Operating system configuration
- B. Application management
- C. Platform management
- D. Code encryption

Answer(s): D

Reference:

<https://aws.amazon.com/lambda/security-overview-of-aws-lambda/>

QUESTION: 513

A company wants to be notified when its AWS Cloud costs or usage exceed defined thresholds. Which AWS service will support these requirements?

- A. AWS Budgets
- B. Cost Explorer
- C. AWS CloudTrail
- D. Amazon Macie

Answer(s): A

Reference:

<https://aws.amazon.com/aws-cost-management/aws-budgets/>

QUESTION: 514

Which AWS service provides the ability to host a NoSQL database in the AWS Cloud?

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

Answer(s): B

Reference:

<https://aws.amazon.com/nosql/>

QUESTION: 515

Which AWS service allows customers to purchase unused Amazon EC2 capacity at an often discounted rate?

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

Answer(s): D

Reference:

<https://aws.amazon.com/ec2/spot/>

QUESTION: 516

Which AWS service or feature requires an internet service provider (ISP) and a colocation facility to be implemented?

- A. AWS VPN
- B. Amazon Connect
- C. AWS Direct Connect
- D. Internet gateway

Answer(s): C

Reference:

<https://aws.amazon.com/directconnect/partners/>

QUESTION: 517

Which AWS services offer compute capabilities? (Choose two.)

- A. Amazon EC2
- B. Amazon S3
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Cognito
- E. AWS Lambda

Answer(s): A, E

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/compute-services.html>

QUESTION: 518

Which AWS service can be used to privately store and manage versions of source code?

- A. AWS CodeBuild

- B. AWS CodeCommit
- C. AWS CodePipeline
- D. AWS CodeStar

Answer(s): B

Reference:

<https://docs.aws.amazon.com/codecommit/latest/userguide/welcome.html>

QUESTION: 519

Which AWS service should a cloud practitioner use to identify security vulnerabilities of an AWS account?

- A. AWS Secrets Manager
- B. Amazon Cognito
- C. Amazon Macie
- D. AWS Trusted Advisor

Answer(s): D

Reference:

<https://www.coalfire.com/the-coalfire-blog/march-2019/aws-trusted-advisor-for-security-compliance>

QUESTION: 520

A company wants to ensure its infrastructure is designed for fault tolerance and business continuity in the event of an environmental disruption.

Which AWS infrastructure component should the company replicate across?

- A. Edge locations
- B. Availability Zones
- C. Regions
- D. Amazon Route 53

Answer(s): B

Reference:

https://d36cz9buwru1tt.cloudfront.net/AWS_Building_Fault_Tolerant_Applications.pdf (3)

QUESTION: 521

Which AWS service or feature is used to send both text and email messages from distributed applications?

- A. Amazon Simple Notification Service (Amazon SNS)
- B. Amazon Simple Email Service (Amazon SES)

- C. Amazon CloudWatch alerts
- D. Amazon Simple Queue Service (Amazon SQS)

Answer(s): D

Reference:

<https://aws.amazon.com/sns/faqs/>

QUESTION: 522

Which AWS Cloud design principles can help increase reliability? (Choose two.)

- A. Using monolithic architecture
- B. Measuring overall efficiency
- C. Testing recovery procedures
- D. Adopting a consumption model
- E. Automatically recovering from failure

Answer(s): C, E

Reference:

<https://wa.aws.amazon.com/wat.pillar.reliability.en.html>

QUESTION: 523

A company is planning to launch an ecommerce site in a single AWS Region to a worldwide user base.

Which AWS services will allow the company to reach users and provide low latency and high transfer speeds? (Choose two.)

- A. Application Load Balancer
- B. AWS Global Accelerator
- C. AWS Direct Connect
- D. Amazon CloudFront
- E. AWS Lambda

Answer(s): A, D

Reference:

<https://aws.amazon.com/cloudfront/faqs/>

QUESTION: 524

A company wants to connect to AWS over a private, low-latency connection from its remote office. What is the recommended method to meet these requirements?

- A. Create a VPN tunnel
- B. Connect across the public internet
- C. Use VPC peering to create a connection.

D. Use AWS Direct Connect.

Answer(s): D

Reference:

<https://aws.amazon.com/getting-started/projects/connect-data-center-to-aws/>

QUESTION: 525

Which AWS service can be used to retrieve compliance reports on demand?

- A. AWS Secrets Manager
- B. AWS Artifact
- C. AWS Security Hub
- D. AWS Certificate Manager

Answer(s): B

Reference:

<https://aws.amazon.com/artifact/>

QUESTION: 526

A company has an AWS-hosted website located behind an Application Load Balancer. The company wants to safeguard the website from SQL injection or cross-site scripting.

Which AWS service should the company use?

- A. Amazon GuardDuty
- B. AWS WAF
- C. AWS Trusted Advisor
- D. Amazon Inspector

Answer(s): B

Reference:

<https://aws.amazon.com/waf/faq/>

QUESTION: 527

How should a web application be deployed to ensure high availability in the AWS Cloud?

- A. Deploy multiple instances of the application in multiple Availability Zones.
- B. Deploy multiple instances of the application in a single Availability Zone.
- C. Deploy the application to a compute-optimized Amazon EC2 instance in a single Availability Zone.
- D. Deploy the application in one Amazon EC2 instance in an Auto Scaling group.

Answer(s): A

Reference:

<https://www.betsol.com/blog/how-to-make-high-availability-web-applications-on-amazon-web-services/>

QUESTION: 528

A company is running a self-managed Oracle database directly on Amazon EC2 for its steady-state database. The company wants to reduce compute costs.

Which option should the company use to maximize savings over a 3-year term?

- A. EC2 Dedicated Instances
- B. EC2 Spot Instances
- C. EC2 Reserved Instances
- D. EC2 On-Demand Instances

Answer(s): C**Reference:**

<https://aws.amazon.com/choosing-a-cloud-platform/>

QUESTION: 529

An external auditor has requested that a company provide a list of all its IAM users, including the status of users' credentials and access keys.

What is the SIMPLEST way to provide this information?

- A. Create an IAM user account for the auditor, granting the auditor administrator permissions.
- B. Take a screenshot of each user's page in the AWS Management Console, then provide the screenshots to the auditor.
- C. Download the IAM credential report, then provide the report to the auditor.
- D. Download the AWS Trusted Advisor report, then provide the report to the auditor.

Answer(s): C**Reference:**

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

QUESTION: 530

What are the benefits of consolidated billing for AWS Cloud services? (Choose two.)

- A. Volume discounts
- B. A minimal additional fee for use
- C. One bill for multiple accounts
- D. Installment payment options
- E. Custom cost and usage budget creation

Answer(s): C, E

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION: 531

A company is expecting a short-term spike in internet traffic for its application. During the traffic increase, the application cannot be interrupted. The company also needs to minimize cost and maximize flexibility.

Which Amazon EC2 instance type should the company use to meet these requirements?

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

Answer(s): B**Reference:**

<https://aws.amazon.com/ec2/faqs/>

QUESTION: 532

A company wants to track AWS resource configuration changes for compliance reasons. Which AWS feature can be used to meet this requirement?

- A. AWS Cost and Usage Report
- B. AWS Organizations service control policies (SCPs)
- C. AWS Config rules
- D. VPC Flow Logs

Answer(s): C**Reference:**

<https://aws.amazon.com/config/>

QUESTION: 533

A company is building an application that needs to deliver images and videos globally with minimal latency. Which approach can the company use to accomplish this in a cost effective manner?

- A. Deliver the content through Amazon CloudFront.
- B. Store the content on Amazon S3 and enable S3 cross-region replication.
- C. Implement a VPN across multiple AWS Regions.
- D. Deliver the content through AWS PrivateLink.

Answer(s): A

Reference:

<https://aws.amazon.com/blogs/industries/how-to-build-a-global-scalable-low-latency-and-secure-machine-learning-medical-imaging-analysis-platform-on-aws/>

QUESTION: 534

The AWS IAM best practice for granting least privilege is to:

- A. apply an IAM policy to an IAM group and limit the size of the group.
- B. require multi-factor authentication (MFA) for all IAM users.
- C. require each IAM user who has different permissions to have multiple passwords.
- D. apply an IAM policy only to IAM users who require it.

Answer(s): D**Reference:**

<https://kirkpatrickprice.com/blog/best-practices-for-privilege-management-in-aws/>

QUESTION: 535

Which cloud computing benefit does AWS demonstrate with its ability to offer lower variable costs as a result of high purchase volumes?

- A. Pay-as-you-go pricing
- B. High availability
- C. Global reach
- D. Economies of scale

Answer(s): D**Reference:**

<https://innovationtactics.com/amazon-business-model-amazon-web-services/>

QUESTION: 536

A pharmaceutical company operates its infrastructure in a single AWS Region. The company has thousands of VPCs in various AWS accounts that it wants to interconnect.

Which AWS service or feature should the company use to help simplify management and reduce operational costs?

- A. VPC endpoint
- B. AWS Direct Connect
- C. AWS Transit Gateway
- D. VPC peering

Answer(s): C**Reference:**

<https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf> (9)

QUESTION: 537

How can AWS enable a company to control expenses as an application's usage changes unpredictably?

- A. AWS will refund the cost difference if a customer moves to larger servers.
- B. The application can be built to scale up or down automatically as resources are needed
- C. Spot instances will automatically be used if the price is lower than on-demand instances.
- D. Amazon CloudWatch will automatically predict what resources are needed.

Answer(s): B**QUESTION: 538**

Which AWS service or feature can be used to prevent SQL injection attacks?

- A. Security groups
- B. Network ACLs
- C. AWS WAF
- D. IAM policy

Answer(s): C**Reference:**

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-sql-conditions.html>

QUESTION: 539

Which AWS service can help a company detect an outage of its website servers and redirect users to alternate servers?

- A. Amazon CloudFront
- B. Amazon GuardDuty
- C. Amazon Route 53
- D. AWS Trusted Advisor

Answer(s): C**Reference:**

<https://aws.amazon.com/about-aws/whats-new/2013/02/11/announcing-dns-failover-for-route-53/>

QUESTION: 540

Which of the following IT tasks does AWS perform to offload a company's IT resource management responsibilities? (Choose two.)

- A. Configuring operating system firewalls
- B. Setting up access controls for data
- C. Backing up databases
- D. Configuring database user accounts
- E. Installing operating systems

Answer(s): C, E

QUESTION: 541

According to security best practices, how should an Amazon EC2 instance be given access to an Amazon S3 bucket?

- A. Hard code an IAM user's secret key and access key directly in the application, and upload the file.
- B. Store the IAM user's secret key and access key in a text file on the EC2 instance, read the keys, then upload the file.
- C. Have the EC2 instance assume a role to obtain the privileges to upload the file.
- D. Modify the S3 bucket policy so that any service can upload to it at any time.

Answer(s): C

QUESTION: 542

A user can increase operational efficiency in the AWS Cloud by:

- A. leveraging AWS managed services.
- B. right-sizing AWS infrastructure.
- C. manually creating all necessary resources.
- D. managing their own software license.

Answer(s): A

Reference:

<https://www.ibexlabs.com/improve-operational-efficiency-via-digital-transformation-on-aws/>

QUESTION: 543

Which AWS service automatically handles application health monitoring?

- A. Amazon API Gateway
- B. AWS Elastic Beanstalk
- C. AWS Lambda
- D. AWS Config

Answer(s): B

Reference:

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

QUESTION: 544

Under the AWS shared responsibility model, which task is the customer's responsibility when managing AWS Lambda functions?

- A. Creating versions of Lambda functions
- B. Maintaining server and operating systems
- C. Scaling Lambda resources according to demand
- D. Updating the Lambda runtime environment

Answer(s): C

QUESTION: 545

A company needs to track the activity in its AWS accounts, and needs to know when an API call is made against its AWS resources.

Which AWS tool or service can be used to meet these requirements?

- A. Amazon CloudWatch
- B. Amazon Inspector
- C. AWS Cloud Trail
- D. AWS IAM

Answer(s): C

Reference:

<https://aws.amazon.com/cloudtrail/>

QUESTION: 546

According to the AWS shared responsibility model, which of the following are AWS responsibilities? (Choose two.)

- A. Network infrastructure and virtualization of infrastructure
- B. Security of application data
- C. Guest operating systems
- D. Physical security of hardware
- E. Credentials and policies

Answer(s): A, D

QUESTION: 547

Which of the following services can be used to block network traffic to an instance? (Choose two.)

- A. Security groups

- B. Amazon Virtual Private Cloud (Amazon VPC) flow logs
- C. Network ACLs
- D. Amazon CloudWatch
- E. AWS CloudTrail

Answer(s): A, C

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-block-or-allow-ips/>

QUESTION: 548

A company wants to transfer petabytes of data as quickly as possible from on-premises locations to the AWS Cloud. Which AWS service should the company use?

- A. AWS Snowball
- B. AWS Global Accelerator
- C. Amazon S3 Transfer Acceleration
- D. Amazon Connect

Answer(s): A

Reference:

<https://aws.amazon.com/getting-started/projects/migrate-petabyte-scale-data/>

QUESTION: 549

A company has refined its workload to use specific AWS services to improve efficiency and reduce cost. Which best practice for cost governance does this example show?

- A. Resource controls
- B. Cost allocation
- C. Architecture optimization
- D. Tagging enforcement

Answer(s): B

Reference:

<https://d1.awsstatic.com/whitepapers/architecture/AWS-Cost-Optimization-Pillar.pdf>

QUESTION: 550

A company hosts images in an Amazon S3 bucket for a public-facing website that is viewed by millions of users around the globe.

Which AWS service will deliver this content with reduced latency?

- A. AWS WAF
- B. Amazon CloudWatch
- C. Amazon CloudFront
- D. AWS CloudFormation

Answer(s): C**Reference:**

<https://aws.amazon.com/getting-started/hands-on/deliver-content-faster/>

QUESTION: 551

Which of the following is an AWS best practice for managing an AWS account root user?

- A. Keep the root user password with the security team.
- B. Enable multi-factor authentication (MFA) for the root user.
- C. Create an access key for the root user.
- D. Keep the root user password consistent for compliance purposes.

Answer(s): B**Reference:**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

QUESTION: 552

A company wants to securely access an Amazon S3 bucket from an Amazon EC2 instance without accessing the internet.

What should the company use to accomplish this goal?

- A. VPN connection
- B. Internet gateway
- C. VPC endpoint
- D. NAT gateway

Answer(s): C**Reference:**

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-instance-access-s3-bucket/>

QUESTION: 553

Which statement is true about AWS global infrastructure?

- A. Availability Zones can span multiple AWS Regions.
- B. A VPC can have different subnets in different AWS Regions.
- C. AWS Regions consist of multiple Availability Zones.
- D. A single subnet can span multiple Availability Zones.

Answer(s): C**Reference:**

<https://digitalcloud.training/certification-training/aws-certified-cloud-practitioner/aws-global-infrastructure/>

QUESTION: 554

Which AWS service or feature provides information about ongoing or upcoming scheduled events that can affect an AWS account?

- A. AWS Config
- B. AWS Systems Manager
- C. AWS Personal Health Dashboard
- D. AWS Trusted Advisor

Answer(s): C

Reference:

<https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/>

QUESTION: 555

A bank needs to store recordings of calls made to its contact center for 6 years. The recordings must be accessible within 48 hours from the time they are requested.

Which AWS service will provide a secure and cost-effective solution for retaining these files?

- A. Amazon DynamoDB
- B. Amazon S3 Glacier
- C. Amazon Connect
- D. Amazon ElastiCache

Answer(s): C

Reference:

<https://docs.aws.amazon.com/connect/latest/adminguide/set-up-recordings.html>

QUESTION: 556

A media company wants to distribute video content to millions of users worldwide over the internet. The company wants to use the AWS global network backbone to distribute cached content with low latency and high data transfer speeds.

Which AWS service will meet these requirements?

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. AWS Direct Connect
- D. Amazon Connect

Answer(s): A

Reference:

<https://aws.amazon.com/cloudfront/>

QUESTION: 557

The AWS global infrastructure consists of Regions, Availability Zones, and what else?

- A. VPCs
- B. Data centers
- C. Dark fiber network links
- D. Edge locations

Answer(s): B

Reference:

<https://www.inqdo.com/aws-explained-global-infrastructure/?lang=en>

QUESTION: 558

Which AWS Trusted Advisor feature is available exclusively to users with AWS Business Support or AWS Enterprise Support?

- A. Notification setup
- B. Refresh checks
- C. AWS Support API
- D. Action links

Answer(s): C

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

QUESTION: 559

A company is required to store its data close to its primary users. Which benefit of the AWS Cloud supports this requirement?

- A. Security
- B. High availability
- C. Elasticity
- D. Global footprint

Answer(s): D

QUESTION: 560

Which of the following contribute to total cost of ownership of a workload running in the AWS Cloud? (Choose two.)

- A. Hardware maintenance
- B. Power and cooling
- C. Storage costs

- D. Space for data center
- E. Network costs

Answer(s): B, D

Reference:

<https://www.slideshare.net/AmazonWebServices/optimizing-total-cost-of-ownership-for-the-aws-cloud-36852296>

QUESTION: 561

Using AWS Identity and Access Management (IAM), what can be attached to an Amazon EC2 instance to make service requests?

- A. Group
- B. Role
- C. Policy
- D. Access key

Answer(s): B

Reference:

<https://aws.amazon.com/iam/faqs/>

QUESTION: 562

A company previously lost data that was stored in an on-premises data center. To protect against future loss of data, the company wants to use AWS to automatically launch thousands of its machines in a fully provisioned state in minutes, in a format that supports data restoration.

Which AWS service should the company use to meet these requirements?

- A. AWS Direct Connect
- B. AWS Storage Gateway
- C. CloudEndure Disaster Recovery
- D. AWS Backup

Answer(s): C

Reference: <https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/backup-recovery.pdf> (35)

QUESTION: 563

Which aspect of AWS infrastructure enables global deployment of compute and storage?

- A. Availability Zones
- B. Regions
- C. Tags

D. Resource groups

Answer(s): A

Reference:

<https://cloudacademy.com/blog/aws-global-infrastructure/>

QUESTION: 564

A security officer wants to enable IPsec communications to securely connect users from on-premises networks to AWS. Which AWS service or feature should the officer use?

- A. Amazon VPC
- B. AWS VPN
- C. AWS Direct Connect
- D. Amazon Connect

Answer(s): B

Reference:

<https://aws.amazon.com/vpn/faqs/>

QUESTION: 565

Which of the following can be used to describe infrastructure as code in the AWS Cloud?

- A. AWS CLI
- B. AWS CloudFormation
- C. AWS CodeDeploy
- D. AWS Amplify

Answer(s): B

Reference:

<https://containersonaws.com/introduction/infrastructure-as-code/#:~:text=Infrastructure%20as%20code%20is%20the,as%20code%20is%20AWS%20CloudFormation.>

QUESTION: 566

Which of the following are benefits of running a database on Amazon RDS compared to an on-premises database? (Choose two.)

- A. RDS backups are managed by AWS.
- B. RDS supports any relational database.
- C. RDS has no database engine licensing costs.
- D. RDS database compute capacity can be easily scaled.
- E. RDS inbound traffic control (for example, security groups) is managed by AWS.

Answer(s): A, D

Reference:

<https://www.missioncloud.com/blog/resource-the-advantages-of-running-sql-server-on-aws>

QUESTION: 567

Which AWS service is designed to help users who want to use machine learning for natural language processing (NLP) but do not have experience in machine learning?

- A. Amazon Comprehend
- B. Amazon SageMaker
- C. AWS Deep Learning AMIs (DLAMI)
- D. Amazon Rekognition

Answer(s): A**Reference:**

<https://aws.amazon.com/comprehend/>

QUESTION: 568

Which AWS service or feature allows a user to establish a dedicated network connection between a company's on-premises data center and the AWS Cloud?

- A. AWS Direct Connect
- B. VPC peering
- C. AWS VPN
- D. Amazon Route 53

Answer(s): A**Reference:**

<https://www.stratoscale.com/blog/cloud/build-secure-tunnel-on-prem-data-center-amazon-cloud/#:~:text=AWS%20Direct%20Connect%20allows%20you,that%20provide%20connectivity%20to%20AWS.>

QUESTION: 569

A company needs 24/7 phone, email, and chat access, with a response time of less than 1 hour if a production system has a service interruption.

Which AWS Support plan meets these requirements at the LOWEST cost?

- A. Basic
- B. Developer
- C. Business
- D. Enterprise

Answer(s): C**Reference:**

<https://aws.amazon.com/premiumsupport/plans/>

QUESTION: 570

How can a user achieve high availability for a web application hosted on AWS?

- A. Use a Classic Load Balancer across multiple AWS Regions.
- B. Use an Application Load Balancer across multiple Availability Zones in one AWS Region.
- C. Set up automatic scaling and load balancing with another application instance running on premises.
- D. Use the AWS Region with the highest number of Availability Zones.

Answer(s): B

QUESTION: 571

A company would like to host its MySQL databases on AWS and maintain full control over the operating system, database installation, and configuration.

Which AWS service should the company use to host the databases?

- A. Amazon RDS
- B. Amazon EC2
- C. Amazon DynamoDB
- D. Amazon Aurora

Answer(s): B

Reference:

[https://d1.awsstatic.com/whitepapers/best-practices-for-running-oracle-database-on-aws.pdf?did=wp_card&trk=wp_card_\(06\)](https://d1.awsstatic.com/whitepapers/best-practices-for-running-oracle-database-on-aws.pdf?did=wp_card&trk=wp_card_(06))

QUESTION: 572

What AWS billing support resource is available to all support levels?

- A. AWS Support concierge
- B. AWS Customer Service
- C. AWS technical account manager
- D. AWS Business Support

Answer(s): B

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

QUESTION: 573

Which AWS services help to improve application performance by reducing latency while accessing content globally? (Choose two.)

- A. Amazon CloudFront
- B. AWS VPN
- C. AWS Direct Connect
- D. AWS Global Accelerator
- E. Amazon S3 Glacier

Answer(s): A, D

Reference:

<https://aws.amazon.com/blogs/networking-and-content-delivery/achieve-up-to-60-better-performance-for-internet-traffic-with-aws-global-accelerator/>

QUESTION: 574

Which AWS service provides the ability to quickly run one-time queries on data in Amazon S3?

- A. Amazon EMR
- B. Amazon DynamoDB
- C. Amazon Redshift
- D. Amazon Athena

Answer(s): D

Reference:

<https://aws.amazon.com/athena/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

QUESTION: 575

Which task requires the use of AWS account root account user credentials?

- A. Closing an AWS account
- B. Creating a log file
- C. Modifying IAM user permissions
- D. Deleting IAM users

Answer(s): A

Reference:

<https://docs.aws.amazon.com/general/latest/gr/root-vs-iam.html>

QUESTION: 576

Which AWS service does AWS Snowball Edge natively support?

- A. AWS Server Migration Service (AWS SMS)
- B. Amazon Aurora
- C. AWS Trusted Advisor
- D. Amazon EC2

Answer(s): D

Reference:

<https://aws.amazon.com/blogs/storage/building-a-linux-edge-computing-solution-with-aws-snowball-edge-and-amazon-ec2/>

QUESTION: 577

A company is building a new archiving system on AWS that will store terabytes of data. The company will NOT retrieve the data often.

Which Amazon S3 storage class will MINIMIZE the cost of the system?

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

Answer(s): A

Reference:

<https://aws.amazon.com/s3/faqs/>

QUESTION: 578

Which type of AWS infrastructure deployment puts AWS compute, storage, database, and other select services closer to end users to run latency-sensitive applications?

- A. AWS Regions
- B. Availability Zones
- C. Local Zones
- D. Edge locations

Answer(s): C

Reference:

<https://aws.amazon.com/about-aws/global-infrastructure/localzones/features/#:~:text=AWS%20Local%20Zones%20are%20a,millisecond%20latency%20to%20end-users.>

QUESTION: 579

Which AWS service enables users to monitor for specific phrases, values, or patterns and set up alarms based on metrics?

- A. AWS IQ
- B. Amazon Comprehend
- C. AWS CloudTrail
- D. Amazon CloudWatch Logs

Answer(s): D

Reference:

<https://aws.amazon.com/cloudwatch/features/>

QUESTION: 580

A company wants durable storage for static content and infinitely scalable data storage infrastructure at the lowest cost. Which AWS service should the company choose?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon S3
- C. AWS Storage Gateway
- D. Amazon Elastic File System (Amazon EFS)

Answer(s): B

Reference:

<https://aws.amazon.com/s3/faqs/>

QUESTION: 581

Which cloud computing advantage is a company applying when it uses AWS Regions to increase application availability to users in different countries?

- A. Pay-as-you-go pricing
- B. Capacity forecasting
- C. Economies of scale
- D. Global reach

Answer(s): C

Reference:

https://pages.awscloud.com/rs/112-TZM-766/images/Cloud%20Economics%20Ebook_October%202018.pdf

QUESTION: 582

A user has an AWS account with a Business-level AWS Support plan and needs assistance with handling a production service disruption.

Which action should the user take?

- A. Contact the dedicated AWS technical account manager (TAM).
- B. Contact the dedicated AWS Concierge Support team.
- C. Open a business-critical system down support case.
- D. Open a production system down support case.

Answer(s): D

QUESTION: 583

A company is looking for a way to encrypt data stored on Amazon S3. Which AWS managed service can be used to help to accomplish this?

- A. AWS Certificate Manager (ACM)
- B. AWS Secrets Manager
- C. AWS Resource Access Manager
- D. AWS Key Management Service (AWS KMS)

Answer(s): D

Reference:

<https://www.nakivo.com/blog/amazon-s3-encryption-configuration-overview/>

QUESTION: 584

When a user wants to utilize their existing per-socket, per-core, or per-virtual machine software licenses for a Microsoft Windows server running on AWS, which Amazon EC2 instance type is required?

- A. Spot Instances
- B. Dedicated Instances
- C. Dedicated Hosts
- D. Reserved Instances

Answer(s): C

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/dedicated-hosts-overview.html>

QUESTION: 585

How can consolidated billing within AWS Organizations help lower overall monthly expenses?

- A. By providing a consolidated view of monthly billing across multiple accounts
- B. By pooling usage across multiple accounts to achieve a pricing tier discount
- C. By automating the creation of new accounts through APIs
- D. By leveraging service control policies (SCPs) for centralized service management

Answer(s): A

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/con-bill-blended-rates.html>

QUESTION: 586

A solutions architect needs to maintain a fleet of Amazon EC2 instances so that any impaired instances are replaced with new ones.

Which AWS service should the solutions architect use?

- A. Amazon Elastic Container Service (Amazon ECS)
- B. Amazon GuardDuty
- C. AWS Shield
- D. AWS Auto Scaling

Answer(s): D

Reference:

<https://aws.amazon.com/ec2/autoscaling/faqs/>

QUESTION: 587

An application deployed in the AWS Cloud has unpredictable usage patterns and is running workloads that cannot be interrupted.

What is the MOST cost-effective Amazon EC2 pricing option for this application?

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

Answer(s): D

Reference:

<https://aws.amazon.com/ec2/pricing/>

QUESTION: 588

A company is migrating its on-premises data center to AWS and wants to provide NFS access to its Linux clients. Which AWS service should the company use?

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

Answer(s): B

Reference:

<https://aws.amazon.com/blogs/storage/transferring-files-from-on-premises-to-aws-and-back-without-leaving-your-vpc-using-aws-datasync/>

QUESTION: 589

An application is receiving SQL injection attacks from multiple external resources. Which AWS service or feature can help automate mitigation against these attacks?

- A. AWS WAF
- B. Security groups
- C. Elastic Load Balancer
- D. Network ACL

Answer(s): A

Reference:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-sqlimatch.html>

QUESTION: 590

Which AWS service enables risk auditing of an AWS account by tracking and recording user actions and source IP addresses?

- A. AWS X-Ray
- B. AWS Shield
- C. AWS Trusted Advisor
- D. AWS CloudTrail

Answer(s): D

Reference:

<https://aws.amazon.com/cloudtrail/#:~:text=AWS%20CloudTrail%20is%20a%20service,actions%20across%20your%20AWS%20infrastructure.>

QUESTION: 591

According to the AWS shared responsibility model, which task is the customer's responsibility?

- A. Maintaining the infrastructure needed to run AWS Lambda
- B. Updating the operating system of Amazon DynamoDB instances
- C. Maintaining Amazon S3 infrastructure
- D. Updating the guest operating system on Amazon EC2 instances

Answer(s): D

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/#:~:text=Customers%20are%20responsible%20for%20managing,also%20extends%20to%20IT%20controls.>

QUESTION: 592

A company must process a large amount of data from social media accounts by making graphical queries with high throughput.

Which AWS service will help the company design a cloud architecture that will meet these requirements?

- A. Amazon RDS
- B. Amazon DynamoDB
- C. Amazon Neptune
- D. Amazon Redshift

Answer(s): C

Reference:

<https://aws.amazon.com/neptune/>

QUESTION: 593

Which databases are available on Amazon RDS? (Choose two.)

- A. Sybase
- B. Microsoft SQL Server
- C. IBM Db2
- D. MongoDB
- E. PostgreSQL

Answer(s): D, E

Reference:

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

QUESTION: 594

Under the AWS shared responsibility model, what is the customer's responsibility when using an AWS managed service?

- A. Physical security of the data centers
- B. Server-side encryption
- C. Customer data
- D. Operating system patching

Answer(s): C

Reference:

<https://aws.amazon.com/blogs/security/the-aws-shared-responsibility-model-and-gdpr/>

QUESTION: 595

Which service is an AWS-managed Hadoop framework that makes it easy, fast, and cost-effective to process large amounts of data across dynamically scalable Amazon EC2 instances?

- A. Amazon EMR

- B. Amazon EC2
- C. AWS Elastic Beanstalk
- D. Amazon Redshift

Answer(s): A

Reference:

<https://aws.amazon.com/big-data/what-is-hbase/#:~:text=HBase%20and%20Hadoop%20on%20AWS,across%20dynamically%20scalable%20EC2%20instances>.

QUESTION: 596

A company with AWS Enterprise Support needs help understanding its monthly AWS bill and wants to implement billing best practices.

Which AWS tool or resource is available to accomplish these goals?

- A. Resource tagging
- B. AWS Concierge Support team
- C. AWS Abuse team
- D. AWS Support

Answer(s): D

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf>

QUESTION: 597

A company spends several months upgrading its on-premises infrastructure every few years. The company wants to reduce infrastructure procurement time by migrating to the AWS Cloud.

What is the main benefit of migrating to the AWS Cloud for this use case?

- A. AWS will help move the existing hardware to the AWS data centers.
- B. The company will have increased agility with on-demand access to IT resources.
- C. Enterprise support will be available to help with recurring application installation and setup.
- D. The company will experience less downtime with Multi-AZ deployments.

Answer(s): B

QUESTION: 598

According to the AWS shared responsibility model, when using Amazon RDS, who is responsible for scheduling and performing backups?

- A. AWS is responsible for both tasks.
- B. The customer is responsible for scheduling and AWS is responsible for performing backups.

- C. The customer is responsible for both tasks.
- D. AWS is responsible for scheduling and the user is responsible for performing backups.

Answer(s): C

QUESTION: 599

Which of the following can be used to identify a specific user who stopped an Amazon EC2 instance?

- A. AWS CloudTrail
- B. Amazon Inspector
- C. Amazon CloudWatch
- D. VPC Flow Logs

Answer(s): C

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-system-instance-status-check.html>

QUESTION: 600

A company has a managed IAM policy that does not grant the necessary permissions for users to accomplish required tasks. How can this be resolved?

- A. Enable AWS Shield Advanced
- B. Create a custom IAM policy
- C. Use a third-party web application firewall (WAF) managed rule from the AWS Marketplace
- D. Use AWS Key Management Service (AWS KMS) to create a customer-managed key

Answer(s): B

QUESTION: 601

Which pricing model will interrupt a running Amazon EC2 instance if capacity becomes temporarily unavailable?

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

Answer(s): C

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-fleet.html>

QUESTION: 602

Which security-related task is the responsibility of the customer in the AWS Cloud?

- A. Securing infrastructure at data centers
- B. Maintaining firewall configurations at a hardware level
- C. Maintaining networking among hardware components
- D. Maintaining server-side encryption

Answer(s): D

Reference:

<https://www.missioncloud.com/blog/aws-security-make-sure-your-share-the-responsibility>

QUESTION: 603

Which AWS service acts as a data extract, transform, and load (ETL) tool to make it easy to prepare data for analytics?

- A. Amazon QuickSight
- B. Amazon Athena
- C. AWS Glue
- D. AWS Elastic Beanstalk

Answer(s): C

Reference:

<https://aws.amazon.com/blogs/database/how-to-extract-transform-and-load-data-for-analytic-processing-using-aws-glue-part-2/>

QUESTION: 604

A company recently migrated to AWS and wants to enable intelligent threat protection and continuous monitoring across all of its AWS accounts.

Which AWS service should the company use to achieve this goal?

- A. Amazon Macie
- B. Amazon GuardDuty
- C. AWS Shield
- D. Amazon Detective

Answer(s): B

Reference:

<https://aws.amazon.com/guardduty/>

QUESTION: 605

A user can optimize Amazon EC2 costs by performing which of the following tasks? (Choose two.)

- A. Implementing Auto Scaling groups to add and remove instances based on demand.
- B. Creating a policy to restrict IAM users from creating new instances.
- C. Setting a budget to limit spending on EC2 instances using AWS Budgets.
- D. Purchasing Reserved Instances.
- E. Adding EC2 instances to a second AWS Region that is geographically close to the end users.

Answer(s): B, C

QUESTION: 606

Which AWS services or features help decrease network latency for a globally dispersed user base? (Choose two.)

- A. Amazon VPC
- B. Elastic Load Balancer
- C. Amazon CloudFront
- D. AWS Direct Connect
- E. AWS Global Accelerator

Answer(s): B, D

Reference:

<https://aws.amazon.com/blogs/startups/optimizing-latency-and-bandwidth-for-aws-traffic/>

QUESTION: 607

AWS Trusted Advisor can monitor and provide advice on what characteristics of an AWS account? (Choose two.)

- A. Compliance with security best practices
- B. Application performance
- C. Network utilization
- D. Cost optimization
- E. Compliance status

Answer(s): B, D

Reference:

<https://aws.amazon.com/blogs/startups/optimizing-latency-and-bandwidth-for-aws-traffic/>

QUESTION: 608

Which AWS service would identify if unrestricted access to a resource has been allowed by a security group?

- A. AWS Trusted Advisor
- B. Amazon CloudWatch
- C. VPC Flow Logs
- D. AWS CloudTrail

Answer(s): A

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/>

QUESTION: 609

Which AWS service or component allows inbound traffic from the internet to access a VPC?

- A. Internet gateway
- B. NAT gateway
- C. AWS WAF
- D. VPC peering

Answer(s): A

Reference:

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

QUESTION: 610

Which architecture concept describes the ability to deploy resources on demand and release resources when they are no longer needed?

- A. High availability
- B. Decoupled architecture
- C. Resilience
- D. Elasticity

Answer(s): D

Reference:

<https://wa.aws.amazon.com/wat.concept.elasticity.en.html>

QUESTION: 611

When using Amazon RDS, what is the customer responsible for?

- A. Patching and maintenance of the underlying operating system.
- B. Managing automatic backups of the database.
- C. Controlling network access through security groups.
- D. Replacing failed instances in the event of a hardware failure.

Answer(s): C

QUESTION: 612

Which controls are shared under the AWS shared responsibility model? (Choose two.)

- A. Awareness and training
- B. Patching of Amazon RDS
- C. Configuration management
- D. Physical and environmental controls
- E. Service and communications protection or security

Answer(s): A, C

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/#:~:text=Shared%20Controls%20-%20Controls%20which%20apply,their%20use%20of%20AWS%20services.>

QUESTION: 613

A company has decided to migrate its production workloads to the AWS Cloud. Which actions can help reduce operational costs as part of the migration? (Choose two.)

- A. Reduce overprovisioned instances.
- B. Rehost all third-party licenses on AWS.
- C. Implement a highly available architecture.
- D. Use managed services.
- E. Improve application security.

Answer(s): D, E

QUESTION: 614

Which design principles are enabled by the AWS Cloud to improve the operation of workloads? (Choose two.)

- A. Minimize upfront design
- B. Loose coupling
- C. Disposable resources
- D. Server design and concurrency
- E. Minimal viable product

Answer(s): B, C

QUESTION: 615

To optimize costs and resource usage, a company needs to monitor the operational health of its entire system of AWS Cloud resources. Which AWS service will meet these requirements?

- A. AWS Organizations
- B. Amazon CloudWatch
- C. AWS CloudTrail

D. AWS Config

Answer(s): B

Reference:

<https://aws.amazon.com/aws-cost-management/aws-cost-optimization/monitor-track-and-analyze/>

QUESTION: 616

If a user has an AWS account with an Enterprise-level AWS Support plan, who is the primary point of contact for billing or account inquiries?

- A. Solutions architect
- B. AWS Concierge Support team
- C. An AWS Marketplace seller
- D. AWS Partner Network (APN) partner

Answer(s): B

QUESTION: 617

Which AWS service will track user activity on AWS?

- A. Amazon GuardDuty
- B. AWS Trusted Advisor
- C. AWS CloudTrail
- D. Amazon CloudWatch

Answer(s): C

Reference:

<https://aws.amazon.com/cloudtrail/#:~:text=Track%20user%20activity%20and%20API%20usage&text=AWS%20CloudTrail%20is%20a%20service,actions%20across%20your%20AWS%20infrastructure.>

QUESTION: 618

A cloud practitioner needs an effective method to decrease application latency and increase performance for end users. Which services will help? (Choose two.)

- A. Amazon Elastic Container Service (Amazon ECS) for Kubernetes
- B. Amazon S3
- C. Amazon AppStream 2.0
- D. Amazon ElastiCache
- E. Amazon CloudFront

Answer(s): D, E

Reference:

<https://aws.amazon.com/blogs/database/latency-reduction-of-hybrid-architectures-with-amazon-elasticache/>

QUESTION: 619

A company is building a business intelligence solution and wants to use dashboards for reporting purposes. Which AWS service can be used?

- A. Amazon Redshift
- B. Amazon Elasticsearch Service (Amazon ES)
- C. Amazon QuickSight
- D. Amazon Athena

Answer(s): C**Reference:**

<https://aws.amazon.com/getting-started/hands-on/create-business-intelligence-dashboards-using-amazon-quicksight/>

QUESTION: 620

A company needs to transfer a large volume of data from an on-premises data center to the AWS Cloud. The company's internet connectivity is slow and unreliable.

Which AWS service can facilitate this data transfer?

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

Answer(s): B**Reference:**

<https://aws.amazon.com/getting-started/projects/migrate-petabyte-scale-data/services-costs/#:~:text=Description%3A%20Snowball%20is%20a%20petabyte,transfer%20times%2C%20and%20security%20concerns.>

QUESTION: 621

A security officer wants a list of any potential vulnerabilities in Amazon EC2 security groups. Which AWS service should the officer use?

- A. Amazon GuardDuty
- B. AWS Trusted Advisor
- C. AWS CloudTrail
- D. AWS Artifact

Answer(s): B

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/>

QUESTION: 622

A company has multiple departments. Each department uses its own AWS account.

Which AWS service or tool can the company use to combine the billing for all accounts into one bill?

- A. Amazon Forecast
- B. AWS Budgets
- C. AWS Organizations
- D. AWS Marketplace

Answer(s): C

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

QUESTION: 623

A cloud practitioner needs to obtain AWS compliance reports before migrating an environment to the AWS Cloud. How can these reports be generated?

- A. Contact the AWS Compliance team
- B. Download the reports from AWS Artifact
- C. Open a case with AWS Support
- D. Generate the reports with Amazon Macie

Answer(s): A

QUESTION: 624

A large company has a workload that requires hardware to remain on premises. The company wants to use the same management and control plane services that it currently uses on AWS. Which AWS service should the company use to meet these requirements?

- A. AWS Device Farm
- B. AWS Fargate
- C. AWS Outposts
- D. AWS Ground Station

Answer(s): C

Reference:

<https://aws.amazon.com/outposts/>

QUESTION: 625

Which tasks require using AWS account root user credentials? (Choose two.)

- A. Creating an Amazon EC2 key pair
- B. Removing an IAM user from the administrators group
- C. Changing the AWS Support plan
- D. Creating an Amazon CloudFront key pair
- E. Granting an IAM user full administrative access

Answer(s): C, E

Reference:

<https://docs.aws.amazon.com/general/latest/gr/root-vs-iam.html>

QUESTION: 626

Which of the following are advantages of using Amazon EC2 instances over traditional on-premises servers? (Choose two.)

- A. Pay-as-you-go pricing
- B. Automation
- C. Self-maintenance of servers
- D. Agility
- E. Access to physical hosts

Answer(s): B, D

QUESTION: 627

To avoid malicious compute activities, a user needs a quick way to determine if any Amazon EC2 instances have ports that allow unrestricted access.

Which AWS service will support this requirement?

- A. VPC Flow Logs
- B. AWS WAF
- C. AWS CloudTrail
- D. AWS Trusted Advisor

Answer(s): D

Reference:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/>

QUESTION: 628

What are the market advantages of running workloads in the AWS Cloud? (Choose two.)

- A. Less staff time is required to deploy new workloads.
- B. Increased time to market for new application features.

- C. Higher acquisition costs to support peak workloads.
- D. Increased productivity for application development teams.
- E. A decrease in the average server CPU utilization.

Answer(s): D, E

Reference:

https://pages.awscloud.com/rs/112-TZM-766/images/GEN_windows-on-aws-it-staff-productivity-idc-mini-report_Sep-2019.pdf

QUESTION: 629

Which Amazon S3 storage class allows users to store data backups for long periods of time at the **LOWEST** cost?

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

Answer(s): C

Reference:

<https://aws.amazon.com/s3/storage-classes/#:~:text=S3%20Glacier%20Deep%20Archive%20is,or%20twice%20in%20a%20year>.

QUESTION: 630

Which of the following technologies provides a secure network connection from on-premises to AWS?

- A. Virtual Private Network
- B. AWS Snowball
- C. Amazon Virtual Private Cloud (Amazon VPC)
- D. AWS Mobile Hub

Answer(s): C

Reference:

<https://aws.amazon.com/blogs/apn/amazon-vpc-for-on-premises-network-engineers-part-one/>

QUESTION: 631

When comparing AWS Cloud with on-premises Total Cost of Ownership, which expenses must be considered? (Choose two.)

- A. Physical storage hardware
- B. Operating system administration
- C. Network infrastructure of data center

- D. Project management
- E. Database schema development

Answer(s): A, C

QUESTION: 632

A company uses Amazon EC2 infrastructure to host steady-state workloads and needs to achieve significant cost savings.

Which EC2 instance pricing model should the company select?

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

Answer(s): A

Reference:

<https://aws.amazon.com/ec2/pricing/>

QUESTION: 633

Which guideline is a well-architected design principle for building cloud applications?

- A. Keep static data closer to compute resources.
- B. Provision resources for peak capacity.
- C. Design for automated recovery from failure.
- D. Use tightly coupled components.

Answer(s): B

QUESTION: 634

What does the AWS Cloud provide to increase the speed and agility of execution for customers? (Choose two.)

- A. Readily available resources with low provisioning times
- B. Scalable compute capacity
- C. Free Tier services usage
- D. Access to AWS data centers
- E. Lower resource provisioning cost

Answer(s): A, D

Reference:

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

QUESTION: 635

A company believes an unauthorized user copied data from an Amazon S3 bucket to their own account.

Which AWS service will record the actions taken by the user?

- A. Amazon CloudWatch
- B. AWS CloudTrail
- C. AWS Infrastructure Event Management
- D. AWS Systems Manager

Answer(s): B

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>

QUESTION: 636

Which AWS service provides a simple way to set up a new multi-account AWS environment and govern it at scale?

- A. AWS Trusted Advisor
- B. AWS Security Hub
- C. AWS Control Tower
- D. AWS Resource Access Manager

Answer(s): C

Reference:

<https://aws.amazon.com/about-aws/whats-new/2020/04/you-can-now-use-aws-control-tower-to-set-up-new-multi-account-aws-environments-in-aws-organizations/>

QUESTION: 637

How does the AWS global infrastructure offer high availability and fault tolerance to its users?

- A. The AWS infrastructure is made up of multiple AWS Regions within various Availability Zones located in areas that have low flood risk, and are interconnected with low-latency networks and redundant power supplies.
- B. The AWS infrastructure consists of subnets containing various Availability Zones with multiple data centers located in the same geographic location.
- C. AWS allows users to choose AWS Regions and data centers so that users can select the closest data centers in different Regions.
- D. The AWS infrastructure consists of isolated AWS Regions with independent Availability Zones that are connected with low-latency networking and redundant power supplies.

Answer(s): D

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/global-infrastructure.html>

QUESTION: 638

How can moving to the AWS Cloud help users reduce the time dedicated to operating system patching? (Choose two.)

- A. Users can take advantage of managed services on AWS.
- B. Users can outsource operating system patching to the AWS Support team.
- C. AWS Professional Services will upgrade instances to the latest operating system versions.
- D. Users have the ability to use license-included Amazon EC2 instances.
- E. Users can take advantage of AWS Systems Manager features.

Answer(s): A, E

QUESTION: 639

A user has an AWS Business Support plan and requires detailed billing information. Which AWS resource will help?

- A. AWS Concierge Support
- B. AWS Service Catalog
- C. AWS Budgets
- D. AWS Cost and Usage Report

Answer(s): A

Reference:

<https://aws.amazon.com/premiumsupport/faqs/>

QUESTION: 640

A company has enabled billing alerts in its AWS account and wants to receive a notification through Amazon Simple Notification Service (Amazon SNS) whenever its monthly bill exceeds a set amount.

Which AWS service or tool should the company use to achieve this?

- A. Amazon CloudWatch
- B. Cost Explorer
- C. AWS Cost and Usage Report
- D. AWS Pricing Calculator

Answer(s): A

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charge_s_with_cloudwatch.html

QUESTION: 641

A user wants to move legacy applications to the AWS Cloud to reduce the total cost. Which option is the MOST cost-effective according to best practices?

- A. Rewrite the legacy applications in an open-source language, such as Python.
- B. Right-size the Amazon EC2 instances to prevent over-provisioning in terms of compute and memory.
- C. Migrate relational databases to Amazon DynamoDB.
- D. Reserve a data center facility with an upfront payment, which provides an additional discount.

Answer(s): B

QUESTION: 642

According to the AWS shared responsibility model, which task is the responsibility of AWS for workloads running on Amazon EC2?

- A. Updating the physical hardware
- B. Updating the operating system
- C. Updating the database engine
- D. Updating the user data

Answer(s): A

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

QUESTION: 643

A user needs to identify underutilized Amazon Elastic Block Store (Amazon EBS) volumes to reduce costs. Which AWS service or feature will meet this requirement?

- A. AWS CloudTrail
- B. AWS Budgets
- C. AWS Trusted Advisor
- D. AWS Personal Health Dashboard

Answer(s): C

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-storage-optimization/optimizing-amazon-ebs-storage.html>

QUESTION: 644

Which AWS service will help a company identify the user who deleted an Amazon EC2 instance yesterday?

- A. Amazon CloudWatch
- B. AWS Trusted Advisor

- C. AWS CloudTrail
- D. Amazon Inspector

Answer(s): C

Reference:

<https://aws.amazon.com/cloudtrail/>

QUESTION: 645

A company has existing software licenses that it wants to bring to AWS, but the licensing model requires licensing physical cores.

How can the company meet this requirement in the AWS Cloud?

- A. Launch an Amazon EC2 instance with default tenancy.
- B. Launch an Amazon EC2 instance on a Dedicated Host.
- C. Create an On-Demand Capacity Reservation.
- D. Purchase Dedicated Reserved Instances.

Answer(s): A

Reference:

<https://aws.amazon.com/blogs/compute/byol-and-oversubscription/>

QUESTION: 646

A company must keep records of all resource changes that are made through the AWS Management Console and AWS APIs.

Which AWS service should the company use to meet this requirement?

- A. Amazon CloudWatch
- B. AWS CloudTrail
- C. AWS X-Ray
- D. Amazon Inspector

Answer(s): B

Reference:

<https://aws.amazon.com/cloudtrail/>

QUESTION: 647

A company requires an isolated environment within AWS for security purposes. Which action can be taken to accomplish this?

- A. Create a separate Availability Zone to host the resources.
- B. Create a separate VPC to host the resources.
- C. Create a placement group to host the resources.

D. Create an AWS Direct Connect connection between the company and AWS.

Answer(s): B

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/infrastructure-security.html>

QUESTION: 648

A company needs to monitor and forecast AWS costs and usage. The company also must set event-driven alert notifications that occur if spending limits are exceeded.

Which AWS service or tool should the company use to meet these requirements?

- A. AWS Budgets
- B. Amazon CloudWatch
- C. AWS Config
- D. AWS Service Catalog

Answer(s): A

Reference:

<https://aws.amazon.com/aws-cost-management/aws-budgets/>

QUESTION: 649

Which of the following is a best practice for creating policies for IAM users?

- A. Start with a large set of permissions and remove the permissions that are not required.
- B. Use only Amazon managed policies.
- C. Start with a minimum set of permissions and grant additional permissions as necessary.
- D. Attach policies directly to each user individually.

Answer(s): C

QUESTION: 650

A user with an AWS Basic Support plan has determined that illegal activities are being run on their AWS resources. What is the recommended method for the user to report the activity to AWS?

- A. Contact the AWS Concierge Support team.
- B. Contact an AWS technical account manager.
- C. Contact the AWS Abuse team.
- D. Contact the AWS Support team.

Answer(s): C

QUESTION: 651

AWS can relieve a company's IT staff of which of the following IT tasks? (Choose two.)

- A. Patching database software
- B. Storage capacity planning
- C. Creating database schemas
- D. Setting up access controls for data
- E. Writing application code

Answer(s): A, C

QUESTION: 652

A company's security team requires that all Amazon EC2 workloads use approved Amazon Machine Images (AMIs).

Which AWS service should the company use to verify that the EC2 instances are using approved AMIs?

- A. Amazon CloudWatch
- B. Amazon Inspector
- C. AWS Config
- D. AWS Trusted Advisor

Answer(s): C

Reference:

<https://aws.amazon.com/blogs/devops/aws-config-checking-for-compliance-with-new-managed-rule-options/>

QUESTION: 653

Which of the following are benefits of using the AWS Cloud? (Choose two.)

- A. 100% fault tolerance
- B. Total control over underlying infrastructure
- C. Fast provisioning of IT resources
- D. Outsourcing all application coding to AWS
- E. Ability to go global quickly

Answer(s): C, E

QUESTION: 654

Which of the following security-related aspects of running an Amazon Elastic Compute Cloud (Amazon EC2) instance is the responsibility of AWS?

- A. Security of private keys
- B. Hypervisor software updates

- C. Security updates to software running on the instance
- D. Policies controlling instance access

Answer(s): B

QUESTION: 655

Which AWS service aggregates, organizes, and prioritizes security alerts and findings from multiple AWS services?

- A. Amazon Detective
- B. Amazon Inspector
- C. Amazon Macie
- D. AWS Security Hub

Answer(s): D

Reference:

<https://aws.amazon.com/security-hub/?aws-security-hub-blogs.sort-by=item.additionalFields.createdDate&aws-security-hub-blogs.sort-order=desc>

QUESTION: 656

A developer has an AWS account and needs access to another account's test database.

Which AWS service or feature can the developer use to gain access to the test database?

- A. Amazon Macie
- B. Security groups
- C. IAM roles
- D. AWS Trusted Advisor

Answer(s): C

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

QUESTION: 657

Using Amazon Elastic Container Service (Amazon ECS) to break down a monolithic architecture into microservices is an example of:

- A. a loosely coupled architecture.
- B. a tightly coupled architecture.
- C. a stateless architecture.
- D. a stateful architecture.

Answer(s): A

Reference:

<https://aws.amazon.com/blogs/apn/migrating-applications-from-monolithic-to-microservice-on-aws/>

QUESTION: 658

Which service enables customers to audit API calls in their AWS accounts?

- A. AWS CloudTrail
- B. AWS Trusted Advisor
- C. Amazon Inspector
- D. AWS X-Ray

Answer(s): A

Reference:

<https://aws.amazon.com/cloudtrail/>

QUESTION: 659

Which VPC component provides a layer of security at the subnet level?

- A. Security groups
- B. Network ACLs
- C. NAT gateways
- D. Route tables

Answer(s): A

Reference:

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

QUESTION: 660

Which benefit is available for Convertible Reserved Instances but NOT Standard Reserved Instances?

- A. The instances can be exchanged for instances of a different instance size.
- B. The instances can be exchanged for instances of a different instance family.
- C. The instances can be changed to a different Availability Zone.
- D. The instances can be changed to a different AWS Region.

Answer(s): C

Reference:

<https://aws.amazon.com/about-aws/whats-new/2016/09/amazon-ec2-convertible-reserved-instances-and-the-reserved-instance-regional-benefit/>

QUESTION: 661

Which of the following enables users to leverage the power of AWS services programmatically?

- A. AWS Command Line Interface (AWS CLI)
- B. AWS Trusted Advisor
- C. AWS CodeDeploy
- D. AWS Management Console

Answer(s): D

Reference:

<https://aws.amazon.com/blogs/aws/category/aws-management-console/>

QUESTION: 662

Which security credentials are required to run commands by using the AWS Command Line Interface (AWS CLI)?

- A. Access Key ID and Secret Access Key
- B. AWS root user email and password
- C. Amazon Elastic Compute Cloud (Amazon EC2) key pairs
- D. AWS Identity and Access Management (IAM) user name and password

Answer(s): A

Reference:

<https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-quickstart.html>

QUESTION: 663

Which are customer responsibilities when using Amazon EC2? (Choose two.)

- A. Underlying hardware maintenance
- B. File-system-level encryption
- C. Guest operating system firewall configuration
- D. Hypervisor-level software patching
- E. Physical security at data center facilities

Answer(s): C, D

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/?ref=wellarchitected>

QUESTION: 664

A web developer has limited knowledge of AWS networking services such as Amazon VPC, Elastic Load Balancing, and Auto Scaling, but wants to host a highly available web application.

Which AWS service would automatically handle the deployment and reduce the complexity for the developer?

- A. AWS CodeDeploy
- B. AWS Resource Access Manager

- C. AWS Elastic Beanstalk
- D. AWS CloudFormation

Answer(s): C

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

QUESTION: 665

A company wants to route its traffic directly and privately to a VPC without going over the public internet. Which connectivity option provides this capability?

- A. AWS VPN
- B. AWS Direct Connect
- C. VPC NAT gateway
- D. VPC internet gateway

Answer(s): D

Reference:

<https://aws.amazon.com/vpc/faqs/>

QUESTION: 666

A company wants to build an application for a new line of business.

According to the AWS Well-Architected Framework, what design principles should be implemented? (Choose two.)

- A. Consolidate multiple AWS accounts into a single account.
- B. Buy and host hardware in the AWS Cloud.
- C. Decouple the AWS Cloud architecture to break up monolithic deployments.
- D. Move on-premises network hardware to VPCs.
- E. Design elasticity into the AWS Cloud design.

Answer(s): D, E

QUESTION: 667

A company wants to forecast its AWS Cloud costs for the upcoming year by analyzing its past AWS Cloud spending trends. Which AWS service should the company use to meet this requirement?

- A. AWS Control Tower
- B. Cost Explorer
- C. AWS OpsWorks
- D. AWS CloudFormation

Answer(s): B

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-forecast.html>

QUESTION: 668

Which AWS service or feature can help a company determine if it has Amazon S3 buckets that are publicly available?

- A. AWS Service Health Dashboard
- B. Amazon CloudWatch Logs
- C. AWS Trusted Advisor
- D. AWS Service Catalog

Answer(s): C**Reference:**

https://d1.awsstatic.com/product-marketing/S3/Amazon_S3_Security_eBook_2020.pdf

QUESTION: 669

A company's newly launched application is gaining in popularity very quickly. To improve customer service, the company wants to set up a phone number to manage the increasing volume of calls received by the company's support staff.

Which AWS service should be used to meet this requirement?

- A. Amazon Connect
- B. Amazon CloudFront
- C. Amazon DirectConnect
- D. AWS Trusted Advisor

Answer(s): A**Reference:**

<https://docs.aws.amazon.com/connect/latest/adminguide/contact-center-phone-number.html>

QUESTION: 670

Which credentials used to sign in to the AWS Management Console meet security best practices? (Choose two.)

- A. An access key
- B. Multi-factor authentication
- C. X.509 certificates
- D. A secret key
- E. User name and password

Answer(s): B, E**Reference:**

<https://aws.amazon.com/blogs/security/getting-started-follow-security-best-practices-as-you-configure-your-aws-resources/>

QUESTION: 671

Which of the following are ways to improve security on AWS? (Choose two.)

- A. Using AWS Artifact
- B. Granting the broadest permissions to all IAM roles
- C. Running application code with AWS Cloud9
- D. Enabling multi-factor authentication (MFA) with Amazon Cognito
- E. Using AWS Trusted Advisor security checks

Answer(s): D, E

Reference:

<https://aws.amazon.com/blogs/security/top-10-security-items-to-improve-in-your-aws-account/>



Amazon

Exam Questions AWS-SysOps

Amazon AWS Certified SysOps Administrator - Associate

NEW QUESTION 1

- (Topic 1)

Your team is excited about the use of AWS because now they have access to programmable Infrastructure". You have been asked to manage your AWS infrastructure in a manner similar to the way you might manage application code. You want to be able to deploy exact copies of different versions of your infrastructure, stage changes into different environments, revert back to previous versions, and identify what versions are running at any particular time (development, test, QA, production).

Which approach addresses this requirement?

- A. Use cost allocation reports and AWS Opsworks to deploy and manage your infrastructure
- B. Use AWS CloudWatch metrics and alerts along with resource tagging to deploy and manage your infrastructure
- C. Use AWS Beanstalk and a version control system like GIT to deploy and manage your infrastructure
- D. Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructure

Answer: B

Explanation:

Reference:

<http://aws.amazon.com/opsworks/faqs/>

NEW QUESTION 2

- (Topic 1)

A media company produces new video files on-premises every day with a total size of around 100GB after compression. All files have a size of 1 - 2 GB and need to be uploaded to Amazon S3 every night in a fixed time window between 3am and 5am. Current upload takes almost 3 hours, although less than half of the available bandwidth is used.

What step(s) would ensure that the file uploads are able to complete in the allotted time window?

- A. Increase your network bandwidth to provide faster throughput to S3
- B. Upload the files in parallel to S3
- C. Pack all files into a single archive, upload it to S3, then extract the files in AWS
- D. Use AWS Import/Export to transfer the video files

Answer: B

Explanation:

Reference:

<http://aws.amazon.com/importexport/faqs/>

NEW QUESTION 3

- (Topic 1)

What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment if the primary DB instance fails?

- A. The IP of the primary DB instance is switched to the standby DB instance
- B. The RDS (Relational Database Service) DB instance reboots
- C. A new DB instance is created in the standby availability zone
- D. The canonical name record (CNAME) is changed from primary to standby

Answer: D

NEW QUESTION 4

- (Topic 1)

How can the domain's zone apex for example "myzone.apexdomain.com" be pointed towards an Elastic Load Balancer?

- A. By using an AAAA record
- B. By using an A record
- C. By using an Amazon Route 53 CNAME record
- D. By using an Amazon Route 53 Alias record

Answer: D

Explanation:

Reference:

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

NEW QUESTION 5

- (Topic 1)

You are tasked with setting up a cluster of EC2 instances for a NoSQL database. The database requires random read IO disk performance up to a 100,000 IOPS at 4KB block size per node.

Which of the following EC2 instances will perform the best for this workload?

- A. A High-Memory Quadruple Extra Large (m2.4xlarge) with EBS-Optimized set to true and a PIOPs EBS volume
- B. A Cluster Compute Eight Extra Large (cc2.8xlarge) using instance storage
- C. High I/O Quadruple Extra Large (hi1.4xlarge) using instance storage
- D. A Cluster GPU Quadruple Extra Large (cg1.4xlarge) using four separate 4000 PIOPS EBS volumes in a RAID 0 configuration

Answer: C

Explanation:

Explanation: Reference:
<http://aws.amazon.com/ec2/instance-types/>

NEW QUESTION 6

- (Topic 1)

You use S3 to store critical data for your company. Several users within your group currently have full permissions to your S3 buckets. You need to come up with a solution that does not impact your users and also protect against the accidental deletion of objects.

Which two options will address this issue? Choose 2 answers

- A. Enable versioning on your S3 Buckets
- B. Configure your S3 Buckets with MFA delete
- C. Create a Bucket policy and only allow read only permissions to all users at the bucket level
- D. Enable object life cycle policies and configure the data older than 3 months to be archived in Glacier

Answer: AB

NEW QUESTION 7

- (Topic 1)

You have been asked to leverage Amazon VPC BC2 and SOS to implement an application that submits and receives millions of messages per second to a message queue. You want to ensure your application has sufficient bandwidth between your EC2 instances and SQS. Which option will provide the most scalable solution for communicating between the application and SQS?

- A. Ensure the application instances are properly configured with an Elastic Load Balancer
- B. Ensure the application instances are launched in private subnets with the EBS-optimized option enabled
- C. Ensure the application instances are launched in public subnets with the associate-public-IP-address=true option enabled
- D. Launch application instances in private subnets with an Auto Scaling group and Auto Scaling triggers configured to watch the SQS queue size

Answer: B

Explanation:

Reference:

<http://www.cardinalpath.com/autoscaling-your-website-with-amazon-web-services-part-2/>

NEW QUESTION 8

- (Topic 1)

You have a web-style application with a stateless but CPU and memory-intensive web tier running on a cc2 8xlarge EC2 instance inside of a VPC. The instance when under load is having problems returning requests within the SLA as defined by your business. The application maintains its state in a DynamoDB table, but the data tier is properly provisioned and responses are consistently fast.

How can you best resolve the issue of the application responses not meeting your SLA?

- A. Add another cc2 8xlarge application instance, and put both behind an Elastic Load Balancer
- B. Move the cc2 8xlarge to the same Availability Zone as the DynamoDB table
- C. Cache the database responses in ElastiCache for more rapid access
- D. Move the database from DynamoDB to RDS MySQL in scale-out read-replica configuration

Answer: B

Explanation:

Reference:

<http://aws.amazon.com/elasticmapreduce/faqs/>

NEW QUESTION 9

- (Topic 1)

You have set up individual AWS accounts for each project. You have been asked to make sure your AWS Infrastructure costs do not exceed the budget set per project for each month.

Which of the following approaches can help ensure that you do not exceed the budget each month?

- A. Consolidate your accounts so you have a single bill for all accounts and projects
- B. Set up auto scaling with CloudWatch alarms using SNS to notify you when you are running too many instances in a given account
- C. Set up CloudWatch billing alerts for all AWS resources used by each project, with a notification occurring when the amount for each resource tagged to a particular project matches the budget allocated to the project
- D. Set up CloudWatch billing alerts for all AWS resources used by each account, with email notifications when it hits 50%, 80% and 90% of its budgeted monthly spend

Answer: C

NEW QUESTION 10

- (Topic 1)

You run a web application where web servers on EC2 instances are in an Auto Scaling group. Monitoring over the last 6 months shows that 6 web servers are necessary to handle the minimum load. During the day up to 12 servers are needed. Five to six days per year, the number of web servers required might go up to 15.

What would you recommend to minimize costs while being able to provide high availability?

- A. 6 Reserved instances (heavy utilization), 6 Reserved instances (medium utilization), rest covered by On-Demand instances
- B. 6 Reserved instances (heavy utilization), 6 On-Demand instances, rest covered by Spot Instances
- C. 6 Reserved instances (heavy utilization) 6 Spot instances, rest covered by On-Demand instances
- D. 6 Reserved instances (heavy utilization) 6 Reserved instances (medium utilization) rest covered by Spot instances

Answer: B

NEW QUESTION 10

- (Topic 1)

You have a web application leveraging an Elastic Load Balancer (ELB) In front of the web servers deployed using an Auto Scaling Group Your database is running

on Relational

Database Service (RDS) The application serves out technical articles and responses to them in general there are more views of an article than there are responses to the article. On occasion, an article on the site becomes extremely popular resulting in significant traffic Increases that causes the site to go down.

What could you do to help alleviate the pressure on the infrastructure while maintaining availability during these events?

Choose 3 answers

- A. Leverage CloudFront for the delivery of the article
- B. Add RDS read-relicas for the read traffic going to your relational database
- C. Leverage ElastiCache for caching the most frequently used dat
- D. Use SQS to queue up the requests for the technical posts and deliver them out of the queu
- E. Use Route53 health checks to fail over to an S3 bucket for an error pag

Answer: ACE

NEW QUESTION 14

- (Topic 1)

You are tasked with the migration of a highly trafficked Node JS application to AWS In order to comply with organizational standards Chef recipes must be used to configure the application servers that host this application and to support application lifecycle events.

Which deployment option meets these requirements while minimizing administrative burden?

- A. Create a new stack within Opsworks add the appropriate layers to the stack and deploy the application
- B. Create a new application within Elastic Beanstalk and deploy this application to a new environment
- C. Launch a Node JS server from a community AMI and manually deploy the application to the launched EC2 instance
- D. Launch and configure Chef Server on an EC2 instance and leverage the AWS CLI to launch application servers and configure those instances using Che

Answer: B

Explanation:

Reference:

<http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deployment.html>

NEW QUESTION 16

- (Topic 1)

You are running a database on an EC2 instance, with the data stored on Elastic Block Store (EBS) for persistence At times throughout the day, you are seeing large variance in the response times of the database queries Looking into the instance with the isolate command you see a lot of wait time on the disk volume that the database's data is stored on.

What two ways can you improve the performance of the database's storage while maintaining the current persistence of the data?

Choose 2 answers

- A. Move to an SSD backed instance
- B. Move the database to an EBS-Optimized Instance
- C. Use Provisioned IOPs EBS
- D. Use the ephemeral storage on an m2 4xiarge Instance Instead

Answer: AB

NEW QUESTION 19

- (Topic 1)

Which of the following requires a custom CloudWatch metric to monitor?

- A. Data transfer of an EC2 instance
- B. Disk usage activity of an EC2 instance
- C. Memory Utilization of an EC2 instance
- D. CPU Utilization of an EC2 instance

Answer: C

Explanation:

Reference:

<http://aws.amazon.com/cloudwatch/>

NEW QUESTION 22

- (Topic 1)

When an EC2 EBS-backed (EBS root) instance is stopped, what happens to the data on any ephemeral store volumes?

- A. Data will be deleted and will no longer be accessible
- B. Data is automatically saved in an EBS volum
- C. Data is automatically saved as an EBS snapshot
- D. Data is unavailable until the instance is restarted

Answer: D

NEW QUESTION 27

- (Topic 1)

Your application currently leverages AWS Auto Scaling to grow and shrink as load increases/decreases and has been performing well. Your marketing team expects a steady ramp up in traffic to follow an upcoming campaign that will result in a 20x growth in traffic over 4 weeks. Your forecast for the approximate number of Amazon EC2 instances necessary to meet the peak demand is 175.

What should you do to avoid potential service disruptions during the ramp up in traffic?

- A. Ensure that you have pre-allocated 175 Elastic IP addresses so that each server will be able to obtain one as it launches
- B. Check the service limits in Trusted Advisor and adjust as necessary so the forecasted count remains within limit
- C. Change your Auto Scaling configuration to set a desired capacity of 175 prior to the launch of the marketing campaign
- D. Pre-warm your Elastic Load Balancer to match the requests per second anticipated during peak demand prior to the marketing campaign

Answer: D

NEW QUESTION 28

- (Topic 1)

If you want to launch Amazon Elastic Compute Cloud (EC2) Instances and assign each instance a predetermined private IP address you should:

- A. Assign a group or sequential Elastic IP address to the instances
- B. Launch the instances in a Placement Group
- C. Launch the instances in the Amazon virtual Private Cloud (VPC).
- D. Use standard EC2 instances since each instance gets a private Domain Name Service (DNS) already
- E. Launch the instance from a private Amazon Machine image (AMI)

Answer: C

Explanation:

Reference:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html>

NEW QUESTION 30

- (Topic 1)

You have an Auto Scaling group associated with an Elastic Load Balancer (ELB). You have noticed that instances launched via the Auto Scaling group are being marked unhealthy due to an ELB health check, but these unhealthy instances are not being terminated.

What do you need to do to ensure trial instances marked unhealthy by the ELB will be terminated and replaced?

- A. Change the thresholds set on the Auto Scaling group health check
- B. Add an Elastic Load Balancing health check to your Auto Scaling group
- C. Increase the value for the Health check interval set on the Elastic Load Balancer
- D. Change the health check set on the Elastic Load Balancer to use TCP rather than HTTP checks

Answer: B

Explanation:

Reference:

<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-add-elb-healthcheck.html>

Add an Elastic Load Balancing Health Check to your Auto Scaling Group

By default, an Auto Scaling group periodically reviews the results of EC2 instance status to determine the health state of each instance. However, if you have associated your Auto Scaling group with an Elastic Load Balancing load balancer, you can choose to use the Elastic Load Balancing health check. In this case, Auto Scaling determines the health status of your instances by checking the results of both the EC2 instance status check and the Elastic Load Balancing instance health check.

For information about EC2 instance status checks, see [Monitor Instances With Status Checks](#) in the [Amazon EC2 User Guide for Linux Instances](#). For information about Elastic Load Balancing health checks, see [Health Check](#) in the [Elastic Load Balancing Developer Guide](#).

This topic shows you how to add an Elastic Load Balancing health check to your Auto Scaling group, assuming that you have created a load balancer and have registered the load balancer with your Auto Scaling group. If you have not registered the load balancer with your Auto Scaling group, see [Set Up a Scaled and Load-Balanced Application](#).

Auto Scaling marks an instance unhealthy if the calls to the Amazon EC2 action `DescribeInstanceStatus` return any state other than `running`, the system status shows `impaired`, or the calls to Elastic Load Balancing action `DescribeInstanceHealth` returns `OutOfService` in the instance state field.

If there are multiple load balancers associated with your Auto Scaling group, Auto Scaling checks the health state of your EC2 instances by making health check calls to each load balancer. For each call, if the Elastic Load Balancing action returns any state other than `InService`, the instance is marked as unhealthy. After Auto Scaling marks an instance as unhealthy, it remains in that state, even if subsequent calls from other load balancers return an `InService` state for the same instance.

NEW QUESTION 32

- (Topic 1)

Your company is moving towards tracking web page users with a small tracking

image loaded on each page. Currently you are serving this image out of US-East, but are starting to get concerned about the time it takes to load the image for users on the west coast.

What are the two best ways to speed up serving this image?

Choose 2 answers

- A. Use Route 53's Latency Based Routing and serve the image out of US-West-2 as well as US-East-1
- B. Serve the image out through CloudFront
- C. Serve the image out of S3 so that it isn't being served off of your web application tier
- D. Use EBS PIOPs to serve the image faster out of your EC2 instances

Answer: AD

NEW QUESTION 35

- (Topic 1)

When attached to an Amazon VPC which two components provide connectivity with external networks? Choose 2 answers

- A. Elastic IP (EIP)
- B. NAT Gateway (NAT)
- C. Internet Gateway (IGW)
- D. Virtual Private Gateway (VGW)

Answer: CD

NEW QUESTION 40

- (Topic 1)

You have been asked to automate many routine systems administrator backup and recovery activities. Your current plan is to leverage AWS-managed solutions as much as possible and automate the rest with the AWS CLI and scripts.

Which task would be best accomplished with a script?

- A. Creating daily EBS snapshots with a monthly rotation of snapshots
- B. Creating daily RDS snapshots with a monthly rotation of snapshots
- C. Automatically detect and stop unused or underutilized EC2 instances
- D. Automatically add Auto Scaled EC2 instances to an Amazon Elastic Load Balancer

Answer: A

NEW QUESTION 45

- (Topic 1)

What are characteristics of Amazon S3? Choose 2 answers

- A. Objects are directly accessible via a URL
- B. S3 should be used to host a relational database
- C. S3 allows you to store objects of virtually unlimited size
- D. S3 allows you to store virtually unlimited amounts of data
- E. S3 offers Provisioned IOPS

Answer: AD

NEW QUESTION 50

- (Topic 2)

A user is accessing RDS from an application. The user has enabled the Multi AZ feature with the MS SQL RDS DB. During a planned outage how will AWS ensure that a switch from DB to a standby replica will not affect access to the application?

- A. RDS will have an internal IP which will redirect all requests to the new DB
- B. RDS uses DNS to switch over to stand by replica for seamless transition
- C. The switch over changes Hardware so RDS does not need to worry about access
- D. RDS will have both the DBs running independently and the user has to manually switch over

Answer: B

Explanation:

In the event of a planned or unplanned outage of a DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone if the user has enabled Multi AZ. The automatic failover mechanism simply changes the DNS record of the DB instance to point to the standby DB instance. As a result, the user will need to re-establish any existing connections to the DB instance. However, as the DNS is the same, the application can access DB seamlessly.

NEW QUESTION 51

- (Topic 2)

You are managing the AWS account of a big organization. The organization has more than 1000+ employees and they want to provide access to the various services to most of the employees. Which of the below mentioned options is the best possible solution in this case?

- A. The user should create a separate IAM user for each employee and provide access to them as per the policy
- B. The user should create an IAM role and attach STS with the role
- C. The user should attach that role to the EC2 instance and setup AWS authentication on that server
- D. The user should create IAM groups as per the organization's departments and add each user to the group for better access control
- E. Attach an IAM role with the organization's authentication service to authorize each user for various AWS services

Answer: D

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The user is managing an AWS account for an organization that already has an identity system, such as the login system for the corporate network (SSO). In this case, instead of creating individual IAM users or groups for each user who need AWS access, it may be more practical to use a proxy server to translate the user identities from the organization network into the temporary AWS security credentials. This proxy server will attach an IAM role to the user after authentication.

NEW QUESTION 54

- (Topic 2)

A user has created a VPC with CIDR 20.0.0.0/16 with only a private subnet and VPN connection using the VPC wizard. The user wants to connect to the instance in a private subnet over SSH. How should the user define the security rule for SSH?

- A. Allow Inbound traffic on port 22 from the user's network
- B. The user has to create an instance in EC2 Classic with an elastic IP and configure the security group of a private subnet to allow SSH from that elastic IP
- C. The user can connect to a instance in a private subnet using the NAT instance
- D. Allow Inbound traffic on port 80 and 22 to allow the user to connect to a private subnet over the Internet

Answer: A

Explanation:

The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, the user can setup a case with a VPN only subnet (private) which uses VPN access to connect with his data centre. When the user has configured this setup with Wizard, all network connections to the instances in the subnet will come from his data centre. The user has to configure the security group of the private subnet which allows the inbound traffic on SSH (port 22) from the data centre's network range.

NEW QUESTION 58

- (Topic 2)

A system admin is managing buckets, objects and folders with AWS S3. Which of the below mentioned statements is true and should be taken in consideration by the sysadmin?

- A. The folders support only ACL
- B. Both the object and bucket can have an Access Policy but folder cannot have policy
- C. Folders can have a policy
- D. Both the object and bucket can have ACL but folders cannot have ACL

Answer: A

Explanation:

A sysadmin can grant permission to the S3 objects or the buckets to any user or make objects public using the bucket policy and user policy. Both use the JSON-based access policy language. Generally if user is defining the ACL on the bucket, the objects in the bucket do not inherit it and vice versa. The bucket policy can be defined at the bucket level which allows the objects as well as the bucket to be public with a single policy applied to that bucket. It cannot be applied at the object level. The folders are similar to objects with no content. Thus, folders can have only ACL and cannot have a policy.

NEW QUESTION 60

- (Topic 2)

An organization has created 5 IAM users. The organization wants to give them the same login ID but different passwords. How can the organization achieve this?

- A. The organization should create a separate login ID but give the IAM users the same alias so that each one can login with their alias
- B. The organization should create each user in a separate region so that they have their own URL to login
- C. It is not possible to have the same login ID for multiple IAM users of the same account
- D. The organization should create various groups and add each user with the same login ID to different group
- E. The user can login with their own group ID

Answer: C

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. Whenever the organization is creating an IAM user, there should be a unique ID for each user. It is not possible to have the same login ID for multiple users. The names of users, groups, roles, instance profiles must be alphanumeric, including the following common characters: plus (+), equal (=), comma (,), period (.), at (@), and dash (-).

NEW QUESTION 64

- (Topic 2)

A user has created a photo editing software and hosted it on EC2. The software accepts requests from the user about the photo format and resolution and sends a message to S3 to enhance the picture accordingly. Which of the below mentioned AWS services will help make a scalable software with the AWS infrastructure in this scenario?

- A. AWS Glacier
- B. AWS Elastic Transcoder
- C. AWS Simple Notification Service
- D. AWS Simple Queue Service

Answer: D

Explanation:

Amazon Simple Queue Service (SQS) is a fast, reliable, scalable, and fully managed message queuing service. SQS provides a simple and cost-effective way to decouple the components of an application. The user can configure SQS, which will decouple the call between the EC2 application and S3. Thus, the application does not keep waiting for S3 to provide the data.

NEW QUESTION 66

- (Topic 2)

A user is planning to evaluate AWS for their internal use. The user does not want to incur any charge on his account during the evaluation. Which of the below mentioned AWS services would incur a charge if used?

- A. AWS S3 with 1 GB of storage
- B. AWS micro instance running 24 hours daily
- C. AWS ELB running 24 hours a day

D. AWS PIOPS volume of 10 GB size

Answer: D

Explanation:

AWS is introducing a free usage tier for one year to help the new AWS customers get started in Cloud. The free tier can be used for anything that the user wants to run in the Cloud. AWS offers a handful of AWS services as a part of this which includes 750 hours of free micro instances and 750 hours of ELB. It includes the AWS S3 of 5 GB and AWS EBS general purpose volume upto 30 GB. PIOPS is not part of free usage tier.

NEW QUESTION 71

- (Topic 2)

A user is planning to use AWS Cloud formation for his automatic deployment requirements. Which of the below mentioned components are required as a part of the template?

- A. Parameters
- B. Outputs
- C. Template version
- D. Resources

Answer: D

Explanation:

AWS Cloud formation is an application management tool which provides application modelling, deployment, configuration, management and related activities. The template is a JSON-format, text-based file that describes all the AWS resources required to deploy and run an application. It can have option fields, such as Template Parameters, Output, Data tables, and Template file format version. The only mandatory value is Resource. The user can define the AWS services which will be used/ created by this template inside the Resource section

NEW QUESTION 74

- (Topic 2)

A user has created a queue named "myqueue" in US-East region with AWS SQS. The user's AWS account ID is 123456789012. If the user wants to perform some action on this queue, which of the below Queue URL should he use?

- A. <http://sqs.us-east-1.amazonaws.com/123456789012/myqueue>
- B. <http://sqs.amazonaws.com/123456789012/myqueue>
- C. <http://sq>
- D. 123456789012.us-east-1.amazonaws.com/myqueue
- E. <http://123456789012.sq>
- F. us-east-1.amazonaws.com/myqueue

Answer: A

Explanation:

When creating a new queue in SQS, the user must provide a queue name that is unique within the scope of all queues of user's account. If the user creates queues using both the latest WSDL and a previous version, he will have a single namespace for all his queues. Amazon SQS assigns each queue created by user an identifier called a queue URL, which includes the queue name and other components that Amazon SQS determines. Whenever the user wants to perform an action on a queue, he must provide its queue URL. The queue URL for the account id 123456789012 & queue name "myqueue" in US-East-1 region will be <http://sqs.us-east-1.amazonaws.com/123456789012/myqueue>.

NEW QUESTION 79

- (Topic 2)

An organization is planning to use AWS for 5 different departments. The finance department is responsible to pay for all the accounts. However, they want the cost separation for each account to map with the right cost centre. How can the finance department achieve this?

- A. Create 5 separate accounts and make them a part of one consolidate billing
- B. Create 5 separate accounts and use the IAM cross account access with the roles for better management
- C. Create 5 separate IAM users and set a different policy for their access
- D. Create 5 separate IAM groups and add users as per the department's employees

Answer: A

Explanation:

AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. Consolidated billing enables the organization to see a combined view of the AWS charges incurred by each account as well as obtain a detailed cost report for each of the individual AWS accounts associated with the paying account.

NEW QUESTION 80

- (Topic 2)

A root AWS account owner is trying to understand various options to set the permission to AWS S3. Which of the below mentioned options is not the right option to grant permission for S3?

- A. User Access Policy
- B. S3 Object Access Policy
- C. S3 Bucket Access Policy
- D. S3 ACL

Answer: B

Explanation:

Amazon S3 provides a set of operations to work with the Amazon S3 resources. Managing S3 resource access refers to granting others permissions to work with S3. There are three ways the root account owner can define access with S3: S3 ACL: The user can use ACLs to grant basic read/write permissions to other AWS accounts. S3 Bucket Policy: The policy is used to grant other AWS accounts or IAM users permissions for the bucket and the objects in it. User Access Policy: Define an IAM user and assign him the IAM policy which grants him access to S3.

NEW QUESTION 83

- (Topic 2)

A user is running one instance for only 3 hours every day. The user wants to save some cost with the instance. Which of the below mentioned Reserved Instance categories is advised in this case?

- A. The user should not use RI; instead only go with the on-demand pricing
- B. The user should use the AWS high utilized RI
- C. The user should use the AWS medium utilized RI
- D. The user should use the AWS low utilized RI

Answer: A

Explanation:

The AWS Reserved Instance provides the user with an option to save some money by paying a one-time fixed amount and then save on the hourly rate. It is advisable that if the user is having 30% or more usage of an instance per day, he should go for a RI. If the user is going to use an EC2 instance for more than 2200-2500 hours per year, RI will help the user save some cost. Here, the instance is not going to run for less than 1500 hours. Thus, it is advisable that the user should use the on-demand pricing.

NEW QUESTION 84

- (Topic 2)

An organization has setup consolidated billing with 3 different AWS accounts. Which of the below mentioned advantages will organization receive in terms of the AWS pricing?

- A. The consolidated billing does not bring any cost advantage for the organization
- B. All AWS accounts will be charged for S3 storage by combining the total storage of each account
- C. The EC2 instances of each account will receive a total of 750*3 micro instance hours free
- D. The free usage tier for all the 3 accounts will be 3 years and not a single year

Answer: B

Explanation:

AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. For billing purposes, AWS treats all the accounts on the consolidated bill as one account. Some services, such as Amazon EC2 and Amazon S3 have volume pricing tiers across certain usage dimensions that give the user lower prices when he uses the service more.

NEW QUESTION 87

- (Topic 2)

A user has configured ELB with three instances. The user wants to achieve High Availability as well as redundancy with ELB. Which of the below mentioned AWS services helps the user achieve this for ELB?

- A. Route 53
- B. AWS Mechanical Turk
- C. Auto Scaling
- D. AWS EMR

Answer: A

Explanation:

The user can provide high availability and redundancy for applications running behind Elastic Load Balancer by enabling the Amazon Route 53 Domain Name System (DNS) failover for the load balancers. Amazon Route 53 is a DNS service that provides reliable routing to the user's infrastructure.

NEW QUESTION 88

- (Topic 2)

A user has enabled the Multi AZ feature with the MS SQL RDS database server. Which of the below mentioned statements will help the user understand the Multi AZ feature better?

- A. In a Multi AZ, AWS runs two DBs in parallel and copies the data asynchronously to the replica copy
- B. In a Multi AZ, AWS runs two DBs in parallel and copies the data synchronously to the replica copy
- C. In a Multi AZ, AWS runs just one DB but copies the data synchronously to the standby replica
- D. AWS MS SQL does not support the Multi AZ feature

Answer: C

Explanation:

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. In a Multi-AZ deployment, Amazon RDS automatically

provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption. Note that the high-availability feature is not a scaling solution for read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a read replica.

NEW QUESTION 91

- (Topic 2)

An organization is setting up programmatic billing access for their AWS account. Which of the below mentioned services is not required or enabled when the organization wants to use programmatic access?

- A. Programmatic access
- B. AWS bucket to hold the billing report
- C. AWS billing alerts
- D. Monthly Billing report

Answer: C

Explanation:

AWS provides an option to have programmatic access to billing. Programmatic Billing Access leverages the existing Amazon Simple Storage Service (Amazon S3). APIs. Thus, the user can build applications that reference his billing data from a CSV (comma-separated value) file stored in an Amazon S3 bucket. To enable programmatic access, the user has to first enable the monthly billing report. Then the user needs to provide an AWS bucket name where the billing CSV will be uploaded. The user should also enable the Programmatic access option.

NEW QUESTION 94

- (Topic 2)

A user has stored data on an encrypted EBS volume. The user wants to share the data with his friend's AWS account. How can user achieve this?

- A. Create an AMI from the volume and share the AMI
- B. Copy the data to an unencrypted volume and then share
- C. Take a snapshot and share the snapshot with a friend
- D. If both the accounts are using the same encryption key then the user can share the volume directly

Answer: B

Explanation:

AWS EBS supports encryption of the volume. It also supports creating volumes from existing snapshots provided the snapshots are created from encrypted volumes. If the user is having data on an encrypted volume and is trying to share it with others, he has to copy the data from the encrypted volume to a new unencrypted volume. Only then can the user share it as an encrypted volume data. Otherwise the snapshot cannot be shared.

NEW QUESTION 95

- (Topic 2)

A user has launched an EC2 instance. The user is planning to setup the CloudWatch alarm. Which of the below mentioned actions is not supported by the CloudWatch alarm?

- A. Notify the Auto Scaling launch config to scale up
- B. Send an SMS using SNS
- C. Notify the Auto Scaling group to scale down
- D. Stop the EC2 instance

Answer: B

Explanation:

A user can create a CloudWatch alarm that takes various actions when the alarm changes state. An alarm watches a single metric over the time period that the user has specified, and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The actions could be sending a notification to an Amazon Simple Notification Service topic (SMS, Email, and HTTP end point), notifying the Auto Scaling policy or changing the state of the instance to Stop/Terminate.

NEW QUESTION 96

- (Topic 2)

A root account owner has created an S3 bucket testmycloud. The account owner wants to allow everyone to upload the objects as well as enforce that the person who uploaded the object should manage the permission of those objects. Which is the easiest way to achieve this?

- A. The root account owner should create a bucket policy which allows the IAM users to upload the object
- B. The root account owner should create the bucket policy which allows the other account owners to set the object policy of that bucket
- C. The root account should use ACL with the bucket to allow everyone to upload the object
- D. The root account should create the IAM users and provide them the permission to upload content to the bucket

Answer: C

Explanation:

Each AWS S3 bucket and object has an ACL (Access Control List) associated with it. An ACL is a list of grants identifying the grantee and the permission granted. The user can use ACLs to grant basic read/write permissions to other AWS accounts. ACLs use an Amazon S3-specific XML schema. The user cannot grant permissions to other users in his account. ACLs are suitable for specific scenarios. For example, if a bucket owner allows other AWS accounts to upload objects,

permissions to these objects can only be managed using the object ACL by the AWS account that owns the object.

NEW QUESTION 101

- (Topic 2)

A user has configured ELB with two EBS backed EC2 instances. The user is trying to understand the DNS access and IP support for ELB. Which of the below mentioned statements may not help the user understand the IP mechanism supported by ELB?

- A. The client can connect over IPv4 or IPv6 using Dualstack
- B. ELB DNS supports both IPv4 and IPv6
- C. Communication between the load balancer and back-end instances is always through IPv4
- D. The ELB supports either IPv4 or IPv6 but not both

Answer: D

Explanation:

Elastic Load Balancing supports both Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4). Clients can connect to the user's load balancer using either IPv4 or IPv6 (in EC2-Classic, DNS). However, communication between the load balancer and its back-end instances uses only IPv4. The user can use the Dualstack-prefixed DNS name to enable IPv6 support for communications between the client and the load balancers. Thus, the clients are able to access the load balancer using either IPv4 or IPv6 as their individual connectivity needs dictate.

NEW QUESTION 106

- (Topic 2)

An organization has added 3 of his AWS accounts to consolidated billing. One of the AWS accounts has purchased a Reserved Instance (RI) of a small instance size in the US-East-1a zone. All other AWS accounts are running instances of a small size in the same zone. What will happen in this case for the RI pricing?

- A. Only the account that has purchased the RI will get the advantage of RI pricing
- B. One instance of a small size and running in the US-East-1a zone of each AWS account will get the benefit of RI pricing
- C. Any single instance from all the three accounts can get the benefit of AWS RI pricing if they are running in the same zone and are of the same size
- D. If there are more than one instances of a small size running across multiple accounts in the same zone no one will get the benefit of RI

Answer: C

Explanation:

AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. For billing purposes, consolidated billing treats all the accounts on the consolidated bill as one account. This means that all accounts on a consolidated bill can receive the hourly cost benefit of the Amazon EC2 Reserved Instances purchased by any other account. In this case only one Reserved Instance has been purchased by one account. Thus, only a single instance from any of the accounts will get the advantage of RI. AWS will implement the blended rate for each instance if more than one instance is running concurrently.

NEW QUESTION 110

- (Topic 2)

A user has enabled detailed CloudWatch metric monitoring on an Auto Scaling group. Which of the below mentioned metrics will help the user identify the total number of instances in an Auto Scaling group including pending, terminating and running instances?

- A. GroupTotalInstances
- B. GroupSumInstances
- C. It is not possible to get a count of all the three metrics together
- D. The user has to find the individual number of running, terminating and pending instances and sum it
- E. GroupInstancesCount

Answer: A

Explanation:

CloudWatch is used to monitor AWS as well as the custom services. For Auto Scaling, CloudWatch provides various metrics to get the group information, such as the Number of Pending, Running or Terminating instances at any moment. If the user wants to get the total number of Running, Pending and Terminating instances at any moment, he can use the GroupTotalInstances metric.

NEW QUESTION 114

- (Topic 2)

A sys admin is trying to understand the Auto Scaling activities. Which of the below mentioned processes is not performed by Auto Scaling?

- A. Reboot Instance
- B. Schedule Actions
- C. Replace Unhealthy
- D. Availability Zone Balancing

Answer: A

Explanation:

There are two primary types of Auto Scaling processes: Launch and Terminate, which launch or terminate instances, respectively. Some other actions performed by Auto Scaling are: AddToLoadBalancer, AlarmNotification, HealthCheck, AZRebalance, ReplaceUnHealthy, and ScheduledActions.

NEW QUESTION 117

- (Topic 2)

A user is trying to setup a recurring Auto Scaling process. The user has setup one process to scale up every day at 8 am and scale down at 7 PM. The user is trying to setup another recurring process which scales up on the 1st of every month at 8 AM and scales down the same day at 7 PM. What will Auto Scaling do in this scenario?

- A. Auto Scaling will execute both processes but will add just one instance on the 1st
- B. Auto Scaling will add two instances on the 1st of the month
- C. Auto Scaling will schedule both the processes but execute only one process randomly
- D. Auto Scaling will throw an error since there is a conflict in the schedule of two separate Auto Scaling Processes

Answer: D**Explanation:**

Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. The user can also configure the recurring schedule action which will follow the Linux cron format. As per Auto Scaling, a scheduled action must have a unique time value. If the user attempts to schedule an activity at a time when another existing activity is already scheduled, the call will be rejected with an error message noting the conflict.

NEW QUESTION 122

- (Topic 2)

An organization (Account ID 123412341234) has attached the below mentioned IAM policy to a user. What does this policy statement entitle the user to perform?

```
"Statement": [  
  {  
    "Sid": "AllowUsersAllActionsForCredentials",  
    "Effect": "Allow",  
    "Action": [  
      "iam:*AccessKey*",  
    ],  
    "Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]  
  }  
]
```

- A. 0
- B. 0
- C. 0
- D. 0

Answer: A**Explanation:**

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the organization (Account ID 123412341234) wants some of their users to manage keys (access and secret access keys) of all IAM users, the organization should set the below mentioned policy which entitles the IAM user to modify keys of all IAM users with CLI, SDK or API.

```
"Statement": [  
  {  
    "Sid": "AllowUsersAllActionsForCredentials",  
    "Effect": "Allow",  
    "Action": [  
      "iam:*AccessKey*",  
    ],  
    "Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]  
  }  
]
```

NEW QUESTION 125

- (Topic 2)

A user has launched an EBS backed instance. The user started the instance at 9 AM in the morning. Between 9 AM to 10 AM, the user is testing some script. Thus, he stopped the instance twice and restarted it. In the same hour the user rebooted the instance once. For how many instance hours will AWS charge the user?

- A. 3 hours
- B. 4 hours
- C. 2 hours
- D. 1 hour

Answer: A**Explanation:**

A user can stop/start or reboot an EC2 instance using the AWS console, the Amazon EC2 CLI or the Amazon EC2 API. Rebooting an instance is equivalent to rebooting an operating system. When the instance is rebooted AWS will not charge the user for the extra hours. In case the user stops the instance, AWS does not charge the running cost but charges only the EBS storage cost. If the user starts and stops the instance multiple times in a single hour, AWS will charge the user for every start and stop. In this case, since the instance was rebooted twice, it will cost the user for 3 instance hours.

NEW QUESTION 129

- (Topic 2)

An organization has created 50 IAM users. The organization has introduced a new policy which will change the access of an IAM user. How can the organization

implement this effectively so that there is no need to apply the policy at the individual user level?

- A. Use the IAM groups and add users as per their role to different groups and apply policy to group
- B. The user can create a policy and apply it to multiple users in a single go with the AWS CLI
- C. Add each user to the IAM role as per their organization role to achieve effective policy setup
- D. Use the IAM role and implement access at the role level

Answer: A

Explanation:

With AWS IAM, a group is a collection of IAM users. A group allows the user to specify permissions for a collection of users, which can make it easier to manage the permissions for those users. A group helps an organization manage access in a better way; instead of applying at the individual level, the organization can apply at the group level which is applicable to all the users who are a part of that group.

NEW QUESTION 133

- (Topic 2)

An organization is using AWS since a few months. The finance team wants to visualize the pattern of AWS spending. Which of the below AWS tool will help for this requirement?

- A. AWS Cost Manager
- B. AWS Cost Explorer
- C. AWS CloudWatch
- D. AWS Consolidated Billing

Answer: B

Explanation:

The AWS Billing and Cost Management console includes the Cost Explorer tool for viewing AWS cost data as a graph. It does not charge extra to user for this service. With Cost Explorer the user can filter graphs using resource tags or with services in AWS. If the organization is using Consolidated Billing it helps generate report based on linked accounts. This will help organization to identify areas that require further inquiry. The organization can view trends and use that to understand spend and to predict future costs.

NEW QUESTION 136

- (Topic 2)

A user has a refrigerator plant. The user is measuring the temperature of the plant every 15 minutes. If the user wants to send the data to CloudWatch to view the data visually, which of the below mentioned statements is true with respect to the information given above?

- A. The user needs to use AWS CLI or API to upload the data
- B. The user can use the AWS Import Export facility to import data to CloudWatch
- C. The user will upload data from the AWS console
- D. The user cannot upload data to CloudWatch since it is not an AWS service metric

Answer: A

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. While sending the data the user has to include the metric name, namespace and timezone as part of the request.

NEW QUESTION 140

- (Topic 2)

A user has recently started using EC2. The user launched one EC2 instance in the default subnet in EC2-VPC. Which of the below mentioned options is not attached or available with the EC2 instance when it is launched?

- A. Public IP address
- B. Internet gateway
- C. Elastic IP
- D. Private IP address

Answer: C

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to a user's AWS account. A subnet is a range of IP addresses in the VPC. The user can launch the AWS resources into a subnet. There are two supported platforms into which a user can launch instances: EC2-Classic and EC2-VPC (default subnet). A default VPC has all the benefits of EC2-VPC and the ease of use of EC2-Classic. Each instance that the user launches into a default subnet has a private IP address and a public IP address. These instances can communicate with the internet through an internet gateway. An internet gateway enables the EC2 instances to connect to the internet through the Amazon EC2 network edge.

NEW QUESTION 143

- (Topic 2)

A user is trying to understand AWS SNS. To which of the below mentioned end points is SNS unable to send a notification?

- A. Email JSON
- B. HTTP
- C. AWS SQS
- D. AWS SES

Answer: D

Explanation:

Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, and fully managed push messaging service. Amazon SNS can deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS) queues or to any HTTP endpoint. The user can select one of the following transports as part of the subscription requests: "HTTP", "HTTPS", "Email", "Email-JSON", "SQS", "and SMS".

NEW QUESTION 147

- (Topic 2)

A user has configured a VPC with a new subnet. The user has created a security group. The user wants to configure that instances of the same subnet communicate with each other. How can the user configure this with the security group?

- A. There is no need for a security group modification as all the instances can communicate with each other inside the same subnet
- B. Configure the subnet as the source in the security group and allow traffic on all the protocols and ports
- C. Configure the security group itself as the source and allow traffic on all the protocols and ports
- D. The user has to use VPC peering to configure this

Answer: C

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. AWS provides two features that the user can use to increase security in VPC: security groups and network ACLs. Security groups work at the instance level. If the user is using the default security group it will have a rule which allows the instances to communicate with each other. For a new security group the user has to specify the rule, add it to define the source as the security group itself, and select all the protocols and ports for that source.

NEW QUESTION 152

- (Topic 2)

An organization is using cost allocation tags to find the cost distribution of different departments and projects. One of the instances has two separate tags with the key/ value as "InstanceName/HR", "CostCenter/HR". What will AWS do in this case?

- A. InstanceName is a reserved tag for AWS
- B. Thus, AWS will not allow this tag
- C. AWS will not allow the tags as the value is the same for different keys
- D. AWS will allow tags but will not show correctly in the cost allocation report due to the same value of the two separate keys
- E. AWS will allow both the tags and show properly in the cost distribution report

Answer: D

Explanation:

AWS provides cost allocation tags to categorize and track the AWS costs. When the user applies tags to his AWS resources, AWS generates a cost allocation report as a comma-separated value (CSV file) with the usage and costs aggregated by those tags. Each tag will have a key-value and can be applied to services, such as EC2, S3, RDS, EMR, etc. It is required that the key should be different for each tag. The value can be the same for different keys. In this case since the value is different, AWS will properly show the distribution report with the correct values.

NEW QUESTION 153

- (Topic 2)

A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances. How can the user change it?

- A. Stop one of the instances and change the availability zone
- B. The zone can only be modified using the AWS CLI
- C. From the AWS EC2 console, select the Actions -> Change zones and specify new zone
- D. Create an AMI of the running instance and launch the instance in a separate AZ

Answer: D

Explanation:

With AWS EC2, when a user is launching an instance he can select the availability zone (AZ) at the time of launch. If the zone is not selected, AWS selects it on behalf of the user. Once the instance is launched, the user cannot change the zone of that instance unless he creates an AMI of that instance and launches a new instance from it.

NEW QUESTION 155

- (Topic 3)

A user has created a VPC with a public subnet. The user has terminated all the instances which are part of the subnet. Which of the below mentioned statements is true with respect to this scenario?

- A. The user cannot delete the VPC since the subnet is not deleted
- B. All network interface attached with the instances will be deleted
- C. When the user launches a new instance it cannot use the same subnet
- D. The subnet to which the instances were launched will be deleted

Answer: B

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. When an instance is launched it will have a network interface attached with it. The user cannot delete the subnet until he terminates the instance and deletes the network interface. When the user terminates the instance all the network interfaces attached with it are also deleted.

NEW QUESTION 156

- (Topic 3)

What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment if the primary DB instance fails?

- A. The IP of the primary DB Instance is switched to the standby DB Instance
- B. A new DB instance is created in the standby availability zone
- C. The canonical name record (CNAME) is changed from primary to standby
- D. The RDS (Relational Database Service) DB instance reboot

Answer: D

Explanation:

Reference:

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RebootInstance.html

NEW QUESTION 159

- (Topic 3)

A user has launched an EC2 Windows instance from an instance store backed AMI. The user wants to convert the AMI to an EBS backed AMI. How can the user convert it?

- A. Attach an EBS volume to the instance and unbundle all the AMI bundled data inside the EBS
- B. A Windows based instance store backed AMI cannot be converted to an EBS backed AMI
- C. It is not possible to convert an instance store backed AMI to an EBS backed AMI
- D. Attach an EBS volume and use the copy command to copy all the ephemeral content to the EBS Volume

Answer: B

Explanation:

Generally when a user has launched an EC2 instance from an instance store backed AMI, it can be converted to an EBS backed AMI provided the user has attached the EBS volume to the instance and unbundles the AMI data to it. However, if the instance is a Windows instance, AWS does not allow this. In this case, since the instance is a Windows instance, the user cannot convert it to an EBS backed AMI.

NEW QUESTION 163

- (Topic 3)

An organization has created a Queue named "modularqueue" with SQS. The organization is not performing any operations such as SendMessage, ReceiveMessage, DeleteMessage, GetQueueAttributes, SetQueueAttributes, AddPermission, and RemovePermission on the queue. What can happen in this scenario?

- A. AWS SQS sends notification after 15 days for inactivity on queue
- B. AWS SQS can delete queue after 30 days without notification
- C. AWS SQS marks queue inactive after 30 days
- D. AWS SQS notifies the user after 2 weeks and deletes the queue after 3 week

Answer: B

Explanation:

Amazon SQS can delete a queue without notification if one of the following actions hasn't been performed on it for 30 consecutive days: SendMessage, ReceiveMessage, DeleteMessage, GetQueueAttributes, SetQueueAttributes, AddPermission, and RemovePermission.

NEW QUESTION 167

- (Topic 3)

A sys admin has enabled logging on ELB. Which of the below mentioned fields will not be a part of the log file name?

- A. Load Balancer IP
- B. EC2 instance IP
- C. S3 bucket name
- D. Random string

Answer: B

Explanation:

Elastic Load Balancing access logs capture detailed information for all the requests made to the load balancer. Elastic Load Balancing publishes a log file from each load balancer node at the interval that the user has specified. The load balancer can deliver multiple logs for the same period. Elastic Load Balancing creates log file names in the following format: "{Bucket}/{Prefix}/AWSLogs/{AWS Account ID}/elasticloadbalancing/{Region}/{Year}/{Month}/{Day}/{AWS Account ID}_elasticloadbalancing_{Region}_{Load Balancer Name}_{End Time}_{Load Balancer IP}_{Random String}.log"

NEW QUESTION 170

- (Topic 3)

A user is trying to connect to a running EC2 instance using SSH. However, the user gets an Unprotected Private Key File error. Which of the below mentioned options can be a possible reason for rejection?

- A. The private key file has the wrong file permission
- B. The ppk file used for SSH is read only
- C. The public key file has the wrong permission
- D. The user has provided the wrong user name for the OS login

Answer: A

Explanation:

While doing SSH to an EC2 instance, if you get an Unprotected Private Key File error it means that the private key file's permissions on your computer are too open. Ideally the private key should have the Unix permission of 0400. To fix that, run the command: chmod 0400 /path/to/private.key

NEW QUESTION 174

- (Topic 3)

A user has launched 5 instances in EC2-CLASSIC and attached 5 elastic IPs to the five different instances in the US East region. The user is creating a VPC in the same region. The user wants to assign an elastic IP to the VPC instance. How can the user achieve this?

- A. The user has to request AWS to increase the number of elastic IPs associated with the account
- B. AWS allows 10 EC2 Classic IPs per region; so it will allow to allocate new Elastic IPs to the same region
- C. The AWS will not allow to create a new elastic IP in VPC; it will throw an error
- D. The user can allocate a new IP address in VPC as it has a different limit than EC2

Answer: D

Explanation:

Section: (none)

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. A user can have 5 IP addresses per region with EC2 Classic. The user can have 5 separate IPs with VPC in the same region as it has a separate limit than EC2 Classic.

NEW QUESTION 176

- (Topic 3)

A user has launched an EC2 instance store backed instance in the US-East-1a zone. The user created AMI #1 and copied it to the Europe region. After that, the user made a few updates to the application running in the US-East-1a zone. The user makes an AMI#2 after the changes. If the user launches a new instance in Europe from the AMI #1 copy, which of the below mentioned statements is true?

- A. The new instance will have the changes made after the AMI copy as AWS just copies the reference of the original AMI during the copyin
- B. Thus, the copied AMI will have all the updated data
- C. The new instance will have the changes made after the AMI copy since AWS keeps updating the AMI
- D. It is not possible to copy the instance store backed AMI from one region to another
- E. The new instance in the EU region will not have the changes made after the AMI copy

Answer: D

Explanation:

Within EC2, when the user copies an AMI, the new AMI is fully independent of the source AMI; there is no link to the original (source) AMI. The user can modify the source AMI without affecting the new AMI and vice versa. Therefore, in this case even if the source AMI is modified, the copied AMI of the EU region will not have the changes. Thus, after copy the user needs to copy the new source AMI to the destination region to get those changes.

NEW QUESTION 178

- (Topic 3)

A user has setup a VPC with CIDR 20.0.0.0/16. The VPC has a private subnet (20.0.1.0/24. and a public subnet (20.0.0.0/24.. The user's data centre has CIDR of 20.0.54.0/24 and 20.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?

- A. It will allow traffic communication on both the CIDRs of the data centre
- B. It will not allow traffic with data centre on CIDR 20.1.0.0/24 but allows traffic communication on 20.0.54.0/24
- C. It will not allow traffic communication on any of the data centre CIDRs
- D. It will allow traffic with data centre on CIDR 20.1.0.0/24 but does not allow on 20.0.54.0/24

Answer: D

Explanation:

VPC allows the user to set up a connection between his VPC and corporate or home network data centre. If the user has an IP address prefix in the VPC that overlaps with one of the networks' prefixes, any traffic to the network's prefix is dropped. In this case CIDR 20.0.54.0/24 falls in the VPC's CIDR range of 20.0.0.0/16. Thus, it will not allow traffic on that IP. In the case of 20.1.0.0/24, it does not fall in the VPC's CIDR range. Thus, traffic will be allowed on it.

NEW QUESTION 180

- (Topic 3)

A user is sending the data to CloudWatch using the CloudWatch API. The user is sending data 90 minutes in the future. What will CloudWatch do in this case?

- A. CloudWatch will accept the data
- B. It is not possible to send data of the future
- C. It is not possible to send the data manually to CloudWatch
- D. The user cannot send data for more than 60 minutes in the future

Answer: A

Explanation:

With Amazon CloudWatch, each metric data point must be marked with a time stamp. The user can send the data using CLI but the time has to be in the UTC format. If the user does not provide the time, CloudWatch will take the data received time in the UTC timezone. The time stamp sent by the user can be up to two weeks in the past and up to two hours into the future.

NEW QUESTION 183

- (Topic 3)

Which of the following statements about this S3 bucket policy is true?

```
{
  "Id": "IPAllowPolicy",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mybucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "192.168.100.0/24"
        },
        "NotIpAddress": {
          "aws:SourceIp": "192.168.100.188/32"
        }
      },
      "Principal": {
        "AWS": [
          "*"
        ]
      }
    }
  ]
}
```

- A. Denies the server with the IP address 192.166 100.0 full access to the "mybucket" bucket
- B. Denies the server with the IP address 192.166 100.188 full access to the "mybucket" bucket
- C. Grants all the servers within the 192 168 100 0/24 subnet full access to the "mybucket" bucket
- D. Grants all the servers within the 192 168 100 188/32 subnet full access to the "mybucket" bucket

Answer: C

NEW QUESTION 186

- (Topic 3)

You have a business-to-business web application running in a VPC consisting of an Elastic Load Balancer (ELB), web servers, application servers and a database. Your web application should only accept traffic from pre-defined customer IP addresses.

Which two options meet this security requirement? Choose 2 answers A. Configure web server VPC security groups to allow traffic from your customers' IPs

- A. Configure your web servers to filter traffic based on the ELB's "X-forwarded-for" header
- B. Configure ELB security groups to allow traffic from your customers' IPs and deny all outbound traffic
- C. Configure a VPC NACL to allow web traffic from your customers' IPs and deny all outbound traffic

Answer: AB

NEW QUESTION 189

- (Topic 3)

A user has launched an RDS MySQL DB with the Multi AZ feature. The user has scheduled the scaling of instance storage during maintenance window. What is the correct order of events during maintenance window?

Perform maintenance on standby

Promote standby to primary

Perform maintenance on original primary

Promote original master back as primary

- A. 1, 2, 3, 4
- B. 1, 2, 3
- C. 2, 3, 1, 4

Answer: B

Explanation:

Running MySQL on the RDS DB instance as a Multi-AZ deployment can help the user reduce the impact of a maintenance event, as the Amazon will conduct maintenance by following the steps in the below mentioned order: Perform maintenance on standby Promote standby to primary Perform maintenance on original primary, which becomes the new standby.

NEW QUESTION 191

- (Topic 3)

Which method can be used to prevent an IP address block from accessing public objects in an S3 bucket?

- A. Create a bucket policy and apply it to the bucket
- B. Create a NACL and attach it to the VPC of the bucket
- C. Create an ACL and apply it to all objects in the bucket
- D. Modify the IAM policies of any users that would access the bucket

Answer: A

Explanation:

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

NEW QUESTION 196

- (Topic 3)

In AWS, which security aspects are the customer's responsibility? Choose 4 answers

- A. Controlling physical access to compute resources
- B. Patch management on the EC2 instance's operating system
- C. Encryption of EBS (Elastic Block Storage) volumes
- D. Life-cycle management of IAM credentials
- E. Decommissioning storage devices
- F. Security Group and ACL (Access Control List) settings

Answer: BCEF

NEW QUESTION 197

- (Topic 3)

A user is planning to scale up an application by 8 AM and scale down by 7 PM daily using Auto Scaling. What should the user do in this case?

- A. Setup the scaling policy to scale up and down based on the CloudWatch alarms
- B. The user should increase the desired capacity at 8 AM and decrease it by 7 PM manually
- C. The user should setup a batch process which launches the EC2 instance at a specific time
- D. Setup scheduled actions to scale up or down at a specific time

Answer: A

Explanation:

Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. To configure the Auto Scaling group to scale based on a schedule, the user needs to create scheduled actions. A scheduled action tells Auto Scaling to perform a scaling action at a certain time in the future.

NEW QUESTION 198

- (Topic 3)

A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24. What will happen in this scenario?

- A. The VPC will modify the first subnet CIDR automatically to allow the second subnet IP range
- B. It is not possible to create a subnet with the same CIDR as VPC
- C. The second subnet will be created
- D. It will throw a CIDR overlaps error

Answer: D

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet.

NEW QUESTION 202

- (Topic 3)

A user wants to find the particular error that occurred on a certain date in the AWS MySQL RDS DB. Which of the below mentioned activities may help the user to get the data easily?

- A. It is not possible to get the log files for MySQL RDS
- B. Find all the transaction logs and query on those records
- C. Direct the logs to the DB table and then query that table
- D. Download the log file to DynamoDB and search for the record

Answer: C

Explanation:

The user can view, download, and watch the database logs using the Amazon RDS console, the Command Line Interface (CLI), or the Amazon RDS API. For the MySQL RDS, the user can view the error log, slow query log, and general logs. The user can also view the MySQL logs easily by directing the logs to a database table in the main database and querying that table.

NEW QUESTION 207

- (Topic 3)

A user is collecting 1000 records per second. The user wants to send the data to CloudWatch using the custom namespace. Which of the below mentioned options is recommended for this activity?

- A. Aggregate the data with statistics, such as Min, max, Average, Sum and Sample data and send the data to CloudWatch
- B. Send all the data values to CloudWatch in a single command by separating them with a comma
- C. CloudWatch will parse automatically
- D. Create one csv file of all the data and send a single file to CloudWatch
- E. It is not possible to send all the data in one call
- F. Thus, it should be sent one by one
- G. CloudWatch will aggregate the data automatically

Answer: A

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user can publish data to CloudWatch as single data points or as an aggregated set of data points called a statistic set using the command put-metric-data. It is recommended that when the user is having multiple data points per minute, he should aggregate the data so that it will minimize the number of calls to put-metric-data. In this case it will be single call to CloudWatch instead of 1000 calls if the data is aggregated.

NEW QUESTION 212

- (Topic 3)

A user has created a VPC with public and private subnets using the VPC wizard. The user has not launched any instance manually and is trying to delete the VPC. What will happen in this scenario?

- A. It will not allow to delete the VPC as it has subnets with route tables
- B. It will not allow to delete the VPC since it has a running route instance
- C. It will terminate the VPC along with all the instances launched by the wizard
- D. It will not allow to delete the VPC since it has a running NAT instance

Answer: D

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the Internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance with an elastic IP. If the user is trying to delete the VPC it will not allow as the NAT instance is still running.

NEW QUESTION 216

- (Topic 3)

A user runs the command "dd if=/dev/zero of=/dev/xvdfbs=1M" on a fresh blank EBS volume attached to a Linux instance. Which of the below mentioned activities is the user performing with the command given above?

- A. Creating a file system on the EBS volume
- B. Mounting the device to the instance
- C. Pre warming the EBS volume
- D. Formatting the EBS volume

Answer: C

Explanation:

When the user creates a new EBS volume and is trying to access it for the first time it will encounter reduced IOPS due to wiping or initiating of the block storage. To avoid this as well as achieve the best performance it is required to pre warm the EBS volume. For a blank volume attached with a Linux OS, the "dd" command is used to write to all the blocks on the device. In the command "dd if=/dev/zero of=/dev/xvdfbs=1M" the parameter "if =import file" should be set to one of the Linux virtual devices, such as /dev/zero. The "of=output file" parameter should be set to the drive that the user wishes to warm. The "bs" parameter sets the block size of the write operation; for optimal performance, this should be set to 1 MB.

NEW QUESTION 221

- (Topic 3)

An organization (Account ID 123412341234) has attached the below mentioned IAM policy to a user. What does this policy statement entitle the user to perform?

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Sid": "AllowUsersAllActionsForCredentials",  
    "Effect": "Allow",  
    "Action": [  
      "iam:*LoginProfile",  
      "iam:*AccessKey*",  
      "iam:*SigningCertificate*"  
    ],  
    "Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]  
  }]
```

- A. The policy allows the IAM user to modify all IAM user's credentials using the console, SDK, CLI or APIs
- B. The policy will give an invalid resource error

- C. The policy allows the IAM user to modify all credentials using only the console
D. The policy allows the user to modify all IAM user's password, sign in certificates and access keys using only CLI, SDK or APIs

Answer: D

Explanation:

WS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the organization (Account ID 123412341234) wants some of their users to manage credentials (access keys, password, and sing in certificates) of all IAM users, they should set an applicable policy to that user or group of users. The below mentioned policy allows the IAM user to modify the credentials of all IAM user's using only CLI, SDK or APIs. The user cannot use the AWS console for this activity since he does not have list permission for the IAM users.

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Sid": "AllowUsersAllActionsForCredentials",  
    "Effect": "Allow",  
    "Action": [  
      "iam:*LoginProfile",  
      "iam:*AccessKey*",  
      "iam:*SigningCertificate*"  
    ],  
    "Resource": ["arn:aws:iam::123412341234:user/${aws:username}"]  
  }]  
}
```

Amazon AWS-SysOps : Practice Test

NEW QUESTION 224

- (Topic 3)

The compliance department within your multi-national organization requires that all data for your customers that reside in the European Union (EU) must not leave the EU and also

data for customers that reside in the US must not leave the US without explicit authorization.

What must you do to comply with this requirement for a web based profile management application running on EC2?

- A. Run EC2 instances in multiple AWS Availability Zones in single Region and leverage an Elastic Load Balancer with session stickiness to route traffic to the appropriate zone to create their profile
B. Run EC2 instances in multiple Regions and leverage Route 53's Latency Based Routing capabilities to route traffic to the appropriate region to create their profile
C. Run EC2 instances in multiple Regions and leverage a third party data provider to determine if a user needs to be redirect to the appropriate region to create their profile
D. Run EC2 instances in multiple AWS Availability Zones in a single Region and leverage a third party data provider to determine if a user needs to be redirect to the appropriate zone to create their profile

Answer: C

NEW QUESTION 226

- (Topic 3)

A user has launched an EBS backed EC2 instance in the US-East-1a region. The user stopped the instance and started it back after 20 days. AWS throws up an 'InsufficientInstanceCapacity' error. What can be the possible reason for this?

- A. AWS does not have sufficient capacity in that availability zone
B. AWS zone mapping is changed for that user account
C. There is some issue with the host capacity on which the instance is launched
D. The user account has reached the maximum EC2 instance limit

Answer: A

Explanation:

When the user gets an 'InsufficientInstanceCapacity' error while launching or starting an EC2 instance, it means that AWS does not currently have enough available capacity to service the user request. If the user is requesting a large number of instances, there might not be enough server capacity to host them. The user can either try again later, by specifying a smaller number of instances or changing the availability zone if launching a fresh instance.

NEW QUESTION 227

- (Topic 3)

A sys admin has enabled a log on ELB. Which of the below mentioned activities are not captured by the log?

- A. Response processing time
B. Front end processing time
C. Backend processing time
D. Request processing time

Answer: B

Explanation:

Elastic Load Balancing access logs capture detailed information for all the requests made to the load balancer. Each request will have details, such as client IP, request path, ELB IP, time, and latencies. The time will have information, such as Request Processing time, Backend Processing time and Response Processing time.

NEW QUESTION 231

- (Topic 3)

A user is using Cloudformation to launch an EC2 instance and then configure an application after the instance is launched. The user wants the stack creation of ELB and AutoScaling to wait until the EC2 instance is launched and configured properly. How can the user configure this?

- A. It is not possible that the stack creation will wait until one service is created and launched
- B. The user can use the HoldCondition resource to wait for the creation of the other dependent resources
- C. The user can use the DependentCondition resource to hold the creation of the other dependent resources
- D. The user can use the WaitCondition resource to hold the creation of the other dependent resources

Answer: D

Explanation:

AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. AWS CloudFormation provides a WaitCondition resource which acts as a barrier and blocks the creation of other resources until a completion signal is received from an external source, such as a user application or management system.

NEW QUESTION 233

- (Topic 3)

A user has created an EBS volume of 10 GB and attached it to a running instance. The user is trying to access EBS for first time. Which of the below mentioned options is the correct statement with respect to a first time EBS access?

- A. The volume will show a size of 8 GB
- B. The volume will show a loss of the IOPS performance the first time
- C. The volume will be blank
- D. If the EBS is mounted it will ask the user to create a file system

Answer: B

Explanation:

A user can create an EBS volume either from a snapshot or as a blank volume. If the volume is from a snapshot it will not be blank. The volume shows the right size only as long as it is mounted. This shows that the file system is created. When the user is accessing the volume the AWS EBS will wipe out the block storage or instantiate from the snapshot. Thus, the volume will show a loss of IOPS. It is recommended that the user should pre-warm the EBS before use to achieve better IO.

NEW QUESTION 235

- (Topic 3)

A user is creating a Cloudformation stack. Which of the below mentioned limitations does not hold true for Cloudformation?

- A. One account by default is limited to 100 templates
- B. The user can use 60 parameters and 60 outputs in a single template
- C. The template, parameter, output, and resource description fields are limited to 4096 characters
- D. One account by default is limited to 20 stacks

Answer: A

Explanation:

AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. The limitations given below apply to the Cloudformation template and stack. There are no limits to the number of templates but each AWS CloudFormation account is limited to a maximum of 20 stacks by default. The Template, Parameter, Output, and Resource description fields are limited to 4096 characters. The user can include up to 60 parameters and 60 outputs in a template.

NEW QUESTION 236

- (Topic 3)

When you put objects in Amazon S3, what is the indication that an object was successfully stored?

- A. Each S3 account has a special bucket named_s3_log
- B. Success codes are written to this bucket with a timestamp and checksum
- C. A success code is inserted into the S3 object metadata
- D. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful
- E. Amazon S3 is engineered for 99.99999999% durability
- F. Therefore there is no need to confirm that data was inserted

Answer: B

Explanation:

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPUT.html>

NEW QUESTION 240

- (Topic 3)

A user has created a VPC with the public subnet. The user has created a security group for that VPC. Which of the below mentioned statements is true when a security group is created?

- A. It can connect to the AWS services, such as S3 and RDS by default

- B. It will have all the inbound traffic by default
- C. It will have all the outbound traffic by default
- D. It will by default allow traffic to the internet gateway

Answer: C

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. AWS provides two features the user can use to increase security in VPC: security groups and network ACLs. Security groups work at the instance level while ACLs work at the subnet level. When a user creates a security group with AWS VPC, by default it will allow all the outbound traffic but block all inbound traffic.

NEW QUESTION 241

- (Topic 3)

Amazon EBS snapshots have which of the following two characteristics? (Choose 2.) Choose 2 answers

- A. EBS snapshots only save incremental changes from snapshot to snapshot
- B. EBS snapshots can be created in real-time without stopping an EC2 instance
- C. EBS snapshots can only be restored to an EBS volume of the same size or smaller
- D. EBS snapshots can only be restored and mounted to an instance in the same Availability Zone as the original EBS volume

Answer: AD

NEW QUESTION 246

- (Topic 3)

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

- A. Launch the test and production instances in separate regions and allow region wise access to the group
- B. Define the IAM policy which allows access based on the instance ID
- C. Create an IAM policy with a condition which allows access to only small instances
- D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags

Answer: D

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The user can add conditions as a part of the IAM policies. The condition can be set on AWS Tags, Time, and Client IP as well as on various parameters. If the organization wants the user to access only specific instances he should define proper tags and add to the IAM policy condition.

The sample policy is shown below.

```
"Statement": [  
  {  
    "Action": "ec2:*",  
    "Effect": "Allow",  
    "Resource": "*",  
    "Condition": {  
      "StringEquals": {  
        "ec2:ResourceTag/InstanceType": "Production"  
      }  
    }  
  }  
]
```

NEW QUESTION 249

- (Topic 3)

A user has created a mobile application which makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

- A. The user should create a separate IAM user for each mobile application and provide DynamoDB access with it
- B. The user should create an IAM role with DynamoDB and EC2 access
- C. Attach the role with EC2 and route all calls from the mobile through EC2
- D. The application should use an IAM role with web identity federation which validates calls to DynamoDB with identity providers, such as Google, Amazon, and Facebook
- E. Create an IAM Role with DynamoDB access and attach it with the mobile application

Answer: C

Explanation:

With AWS IAM a user is creating an application which runs on an EC2 instance and makes requests to AWS, such as DynamoDB or S3 calls. Here it is recommended that the user should not create an IAM user and pass the user's credentials to the application or embed those credentials inside the application. If the user is creating an app that runs on a mobile phone and makes requests to AWS, the user should not create an IAM user and distribute the user's access key with the app. Instead, he should use an identity provider, such as Login with Amazon, Facebook, or Google to authenticate the users, and then use that identity to get temporary security credentials.

NEW QUESTION 250

- (Topic 3)

A user has created a subnet in VPC and launched an EC2 instance within it. The user has not selected the option to assign the IP address while launching the instance. The user has 3 elastic IPs and is trying to assign one of the Elastic IPs to the VPC instance from the console. The console does not show any instance in the IP assignment screen. What is a possible reason that the instance is unavailable in the assigned IP console?

- A. The IP address may be attached to one of the instances
- B. The IP address belongs to a different zone than the subnet zone
- C. The user has not created an internet gateway
- D. The IP addresses belong to EC2 Classic; so they cannot be assigned to VPC

Answer: D

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. When the user is launching an instance he needs to select an option which attaches a public IP to the instance. If the user has not selected the option to attach the public IP then it will only have a private IP when launched. If the user wants to connect to an instance from the internet he should create an elastic IP with VPC. If the elastic IP is a part of EC2 Classic it cannot be assigned to a VPC instance.

NEW QUESTION 254

- (Topic 3)

A sys admin is planning to subscribe to the RDS event notifications. For which of the below mentioned source categories the subscription cannot be configured?

- A. DB security group
- B. DB snapshot
- C. DB options group
- D. DB parameter group

Answer: C

Explanation:

Amazon RDS uses the Amazon Simple Notification Service (SNS) to provide a notification when an Amazon RDS event occurs. These events can be configured for source categories, such as DB instance, DB security group, DB snapshot and DB parameter group.

NEW QUESTION 255

- (Topic 3)

A user has configured an HTTPS listener on an ELB. The user has not configured any security policy which can help to negotiate SSL between the client and ELB. What will ELB do in this scenario?

- A. By default ELB will select the first version of the security policy
- B. By default ELB will select the latest version of the policy
- C. ELB creation will fail without a security policy
- D. It is not required to have a security policy since SSL is already installed

Answer: B

Explanation:

Elastic Load Balancing uses a Secure Socket Layer (SSL) negotiation configuration which is known as a Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. If the user has created an HTTPS/SSL listener without associating any security policy, Elastic Load Balancing will, by default, associate the latest version of the ELBSecurityPolicy-YYYY-MM with the load balancer.

NEW QUESTION 258

- (Topic 3)

A user is receiving a notification from the RDS DB whenever there is a change in the DB security group. The user does not want to receive these notifications for only a month. Thus, he does not want to delete the notification. How can the user configure this?

- A. Change the Disable button for notification to "Yes" in the RDS console
- B. Set the send mail flag to false in the DB event notification console
- C. The only option is to delete the notification from the console
- D. Change the Enable button for notification to "No" in the RDS console

Answer: D

Explanation:

Amazon RDS uses the Amazon Simple Notification Service to provide a notification when an Amazon RDS event occurs. Event notifications are sent to the addresses that the user has provided while creating the subscription. The user can easily turn off the notification without deleting a subscription by setting the Enabled radio button to No in the Amazon RDS console or by setting the Enabled parameter to false using the CLI or Amazon RDS API.

NEW QUESTION 262

- (Topic 3)

A user runs the command "dd if=/dev/xvdf of=/dev/null bs=1M" on an EBS volume created from a snapshot and attached to a Linux instance. Which of the below mentioned activities is the user performing with the step given above?

- A. Pre warming the EBS volume
- B. Initiating the device to mount on the EBS volume
- C. Formatting the volume
- D. Copying the data from a snapshot to the device

Answer: A

Explanation:

When the user creates an EBS volume and is trying to access it for the first time it will encounter reduced IOPS due to wiping or initiating of the block storage. To avoid this as well as achieve the best performance it is required to pre warm the EBS volume. For a volume created from a snapshot and attached with a Linux OS, the “dd” command pre warms the existing data on EBS and any restored snapshots of volumes that have been previously fully pre warmed. This command maintains incremental snapshots; however, because this operation is read-only, it does not pre warm unused space that has never been written to on the original volume. In the command “dd if=/dev/xvdf of=/dev/null bs=1M”, the parameter “if=input file” should be set to the drive that the user wishes to warm. The “of=output file” parameter should be set to the Linux null virtual device, /dev/null. The “bs” parameter sets the block size of the read operation; for optimal performance, this should be set to 1 MB.

NEW QUESTION 266

- (Topic 3)

A user is measuring the CPU utilization of a private data centre machine every minute. The machine provides the aggregate of data every hour, such as Sum of data”, “Min value”, “Max value, and “Number of Data points”.

The user wants to send these values to CloudWatch. How can the user achieve this?

- A. Send the data using the put-metric-data command with the aggregate-values parameter
- B. Send the data using the put-metric-data command with the average-values parameter
- C. Send the data using the put-metric-data command with the statistic-values parameter
- D. Send the data using the put-metric-data command with the aggregate –data parameter

Answer: C

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user can publish the data to CloudWatch as single data points or as an aggregated set of data points called a statistic set using the command put-metric-data. When sending the aggregate data, the user needs to send it with the parameter statistic-values: awscloudwatch put-metric-data --metric-name <Name> --namespace <Custom namespace> --timestamp <UTC Format> --statistic-values Sum=XX,Minimum=YY,Maximum=AA,SampleCount=BB --unit Milliseconds

NEW QUESTION 270

- (Topic 3)

An organization has configured Auto Scaling with ELB. There is a memory issue in the application which is causing CPU utilization to go above 90%. The higher CPU usage triggers an event for Auto Scaling as per the scaling policy. If the user wants to find the root cause inside the application without triggering a scaling activity, how can he achieve this?

- A. Stop the scaling process until research is completed
- B. It is not possible to find the root cause from that instance without triggering scaling
- C. Delete Auto Scaling until research is completed
- D. Suspend the scaling process until research is completed

Answer: D

Explanation:

Auto Scaling allows the user to suspend and then resume one or more of the Auto Scaling processes in the Auto Scaling group. This is very useful when the user wants to investigate a configuration problem or some other issue, such as a memory leak with the web application and then make changes to the application, without triggering the Auto Scaling process.

NEW QUESTION 273

- (Topic 3)

George has launched three EC2 instances inside the US-East-1a zone with his AWS account. Ray has launched two EC2 instances in the US-East-1a zone with his AWS account. Which of the below mentioned statements will help George and Ray understand the availability zone (AZ) concept better?

- A. The instances of George and Ray will be running in the same data centre
- B. All the instances of George and Ray can communicate over a private IP with a minimal cost
- C. All the instances of George and Ray can communicate over a private IP without any cost
- D. The US-East-1a region of George and Ray can be different availability zones

Answer: D

Explanation:

Each AWS region has multiple, isolated locations known as Availability Zones. To ensure that the AWS resources are distributed across the Availability Zones for a region, AWS independently maps the Availability Zones to identifiers for each account. In this case the Availability Zone US-East-1a where George's EC2 instances are running might not be the same location as the US-East-1a zone of Ray's EC2 instances. There is no way for the user to coordinate the Availability Zones between accounts.

NEW QUESTION 278

- (Topic 3)

A sys admin is trying to understand the sticky session algorithm. Please select the correct sequence of steps, both when the cookie is present and when it is not, to help the admin understand the implementation of the sticky session:

ELB inserts the cookie in the response ELB chooses the instance based on the load balancing algorithm Check the cookie in the service request The cookie is found in the request The cookie is not found in the request

- A. 3,1,4,2 [Cookie is not Present] & 3,1,5,2 [Cookie is Present]

- B. 3,4,1,2 [Cookie is not Present] & 3,5,1,2 [Cookie is Present]
- C. 3,5,2,1 [Cookie is not Present] & 3,4,2,1 [Cookie is Present]
- D. 3,2,5,4 [Cookie is not Present] & 3,2,4,5 [Cookie is Present]

Answer: C

Explanation:

Generally AWS ELB routes each request to a zone with the minimum load. The Elastic Load Balancer provides a feature called sticky session which binds the user's session with a specific EC2 instance. The load balancer uses a special load-balancer-generated cookie to track the application instance for each request. When the load balancer receives a request, it first checks to see if this cookie is present in the request. If so, the request is sent to the application instance specified in the cookie. If there is no cookie, the load balancer chooses an application instance based on the existing load balancing algorithm. A cookie is inserted into the response for binding subsequent requests from the same user to that application instance.

NEW QUESTION 283

- (Topic 3)

A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling AddToLoadBalancer (which adds instances to the load balancer) process for a while. What will happen to the instances launched during the suspension period?

- A. The instances will not be registered with ELB and the user has to manually register when the process is resumed
- B. The instances will be registered with ELB only once the process has resumed
- C. Auto Scaling will not launch the instance during this period due to process suspension
- D. It is not possible to suspend only the AddToLoadBalancer process

Answer: A

Explanation:

Auto Scaling performs various processes, such as Launch, Terminate, add to Load Balancer etc. The user can also suspend the individual process. The AddToLoadBalancer process type adds instances to the load balancer when the instances are launched. If this process is suspended, Auto Scaling will launch the instances but will not add them to the load balancer. When the user resumes this process, Auto Scaling will resume adding new instances launched after resumption to the load balancer. However, it will not add running instances that were launched while the process was suspended; those instances must be added manually.

NEW QUESTION 285

- (Topic 3)

A user has configured an ELB to distribute the traffic among multiple instances. The user instances are facing some issues due to the back-end servers. Which of the below mentioned CloudWatch metrics helps the user understand the issue with the instances?

- A. HTTPCode_Backend_3XX
- B. HTTPCode_Backend_4XX
- C. HTTPCode_Backend_2XX
- D. HTTPCode_Backend_5XX

Answer: D

Explanation:

CloudWatch is used to monitor AWS as well as the custom services. For ELB, CloudWatch provides various metrics including error code by ELB as well as by back-end servers (instances.. It gives data for the count of the number of HTTP response codes generated by the back-end instances. This metric does not include any response codes generated by the load balancer. These metrics are: The 2XX class status codes represents successful actions The 3XX class status code indicates that the user agent requires action The 4XX class status code represents client errors The 5XX class status code represents back-end server errors

NEW QUESTION 288

- (Topic 3)

A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet. How can the instances in the private subnet connect to the internet?

- A. Use the internet gateway with a private IP
- B. Allow outbound traffic in the security group for port 80 to allow internet updates
- C. The private subnet can never connect to the internet
- D. Use NAT with an elastic IP

Answer: D

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created two subnets (one private and one public), he would need a Network Address Translation (NAT) instance with the elastic IP address. This enables the instances in the private subnet to send requests to the internet (for example, to perform software updates..

NEW QUESTION 289

- (Topic 3)

Which of the below mentioned AWS RDS logs cannot be viewed from the console for MySQL?

- A. Error Log
- B. Slow Query Log
- C. Transaction Log

D. General Log

Answer: C

Explanation:

The user can view, download, and watch the database logs using the Amazon RDS console, the Command Line Interface (CLI., or the Amazon RDS API. For the MySQL RDS, the user can view the error log, slow querylog, and general logs. RDS does not support viewing the transaction logs.

NEW QUESTION 291

- (Topic 3)

An AWS account wants to be part of the consolidated billing of his organization's payee account. How can the owner of that account achieve this?

- A. The payee account has to request AWS support to link the other accounts with his account
- B. The owner of the linked account should add the payee account to his master account list from the billing console
- C. The payee account will send a request to the linked account to be a part of consolidated billing
- D. The owner of the linked account requests the payee account to add his account to consolidated billing

Answer: C

Explanation:

AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS. accounts within a single organization by making a single paying account. To add a particular account (linked. to the master (payee. account, the payee account has to request the linked account to join consolidated billing. Once the linked account accepts the request henceforth all charges incurred by the linked account will be paid by the payee account.

NEW QUESTION 292

- (Topic 3)

A user is trying to connect to a running EC2 instance using SSH. However, the user gets a Host key not found error. Which of the below mentioned options is a possible reason for rejection?

- A. The user has provided the wrong user name for the OS login
- B. The instance CPU is heavily loaded
- C. The security group is not configured properly
- D. The access key to connect to the instance is wrong

Answer: A

Explanation:

If the user is trying to connect to a Linux EC2 instance and receives the Host Key not found error the probable reasons are: The private key pair is not right The user name to login is wrong

NEW QUESTION 297

- (Topic 3)

How can software determine the public and private IP addresses of the Amazon EC2 instance that it is running on?

- A. Query the local instance metadata
- B. Query the appropriate Amazon CloudWatch metrics
- C. Query the local instance user data
- D. Use ipconfig or ifconfig command

Answer: B

NEW QUESTION 300

- (Topic 3)

A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned SSL protocols is not supported by the security policy?

- A. TLS 1.3
- B. TLS 1.2
- C. SSL 2.0
- D. SSL 3.0

Answer: A

Explanation:

Elastic Load Balancing uses a Secure Socket Layer (SSL) negotiation configuration which is known as a Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. Elastic Load Balancing supports the following versions of the SSL protocol: TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.0 SSL 2.0

NEW QUESTION 303

- (Topic 3)

A user has configured ELB with a TCP listener at ELB as well as on the back-end instances. The user wants to enable a proxy protocol to capture the source and destination IP information in the header. Which of the below mentioned statements helps the user understand a proxy protocol with TCP configuration?

- A. If the end user is requesting behind a proxy server then the user should not enable a proxy protocol on ELB
- B. ELB does not support a proxy protocol when it is listening on both the load balancer and the back-end instances
- C. Whether the end user is requesting from a proxy server or directly, it does not make a difference for the proxy protocol
- D. If the end user is requesting behind the proxy then the user should add the "isproxy" flag to the ELB Configuration

Answer: A

Explanation:

When the user has configured Transmission Control Protocol (TCP) or Secure Sockets Layer (SSL) for both front-end and back-end connections of the Elastic Load Balancer, the load balancer forwards the request to the back-end instances without modifying the request headers unless the proxy header is enabled. If the end user is requesting from a Proxy Protocol enabled proxy server, then the ELB admin should not enable the Proxy Protocol on the load balancer. If the Proxy Protocol is enabled on both the proxy server and the load balancer, the load balancer will add another header to the request which already has a header from the proxy server. This duplication may result in errors.

NEW QUESTION 308

- (Topic 3)

A storage admin wants to encrypt all the objects stored in S3 using server side encryption. The user does not want to use the AES 256 encryption key provided by S3. How can the user achieve this?

- A. The admin should upload his secret key to the AWS console and let S3 decrypt the objects
- B. The admin should use CLI or API to upload the encryption key to the S3 bucket
- C. When making a call to the S3 API mention the encryption key URL in each request
- D. S3 does not support client supplied encryption keys for server side encryption
- E. The admin should send the keys and encryption algorithm with each API call

Answer: D

Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key. Amazon S3 never stores the user's encryption key. The user has to supply it for each encryption or decryption call.

NEW QUESTION 310

- (Topic 3)

A .NET application that you manage is running in Elastic Beanstalk. Your developers tell you they will need access to application log files to debug issues that arise. The infrastructure will scale up and down.

How can you ensure the developers will be able to access only the log files?

- A. Access the log files directly from Elastic Beanstalk
- B. Enable log file rotation to S3 within the Elastic Beanstalk configuration
- C. Ask your developers to enable log file rotation in the applications web.config file
- D. Connect to each Instance launched by Elastic Beanstalk and create a Windows Scheduled task to rotate the log files to S3.

Answer: D

Explanation:

Reference:

<http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.loggingS3.title.html>

NEW QUESTION 315

- (Topic 3)

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption (SSE-C), which of the below mentioned statements is true?

- A. The user should use the same encryption key for all versions of the same object
- B. It is possible to have different encryption keys for different versions of the same object
- C. AWS S3 does not allow the user to upload his own keys for server side encryption
- D. The SSE-C does not work when versioning is enabled

Answer: B

Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key (SSE-C). If the bucket is versioning-enabled, each object version uploaded by the user using the SSE-C feature can have its own encryption key. The user is responsible for tracking which encryption key was used for which object's version

NEW QUESTION 319

- (Topic 3)

A user has created an application which will be hosted on EC2. The application makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK to connect with from the EC2 instance. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

- A. The user should attach an IAM role with DynamoDB access to the EC2 instance
- B. The user should create an IAM user with DynamoDB access and use its credentials within the application to connect with DynamoDB
- C. The user should create an IAM role, which has EC2 access so that it will allow deploying the application

- D. The user should create an IAM user with DynamoDB and EC2 access
- E. Attach the user with the application so that it does not use the root account credentials

Answer: A

Explanation:

With AWS IAM a user is creating an application which runs on an EC2 instance and makes requests to AWS, such as DynamoDB or S3 calls. Here it is recommended that the user should not create an IAM user and pass the user's credentials to the application or embed those credentials inside the application. Instead, the user should use roles for EC2 and give that role access to DynamoDB /S3. When the roles are attached to EC2, it will give temporary security credentials to the application hosted on that EC2, to connect with DynamoDB / S3.

NEW QUESTION 324

- (Topic 3)

A user has created a VPC with a subnet and a security group. The user has launched an instance in that subnet and attached a public IP. The user is still unable to connect to the instance. The internet gateway has also been created. What can be the reason for the error?

- A. The internet gateway is not configured with the route table
- B. The private IP is not present
- C. The outbound traffic on the security group is disabled
- D. The internet gateway is not configured with the security group

Answer: A

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. AWS provides two features the user can use to increase security in VPC: security groups and network ACLs. Security groups work at the instance level. When a user launches an instance and wants to connect to an instance, he needs an internet gateway. The internet gateway should be configured with the route table to allow traffic from the internet.

NEW QUESTION 328

- (Topic 3)

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24. and VPN only subnets CIDR (20.0.1.0/24. along with the VPN gateway (vgw-12345. to connect to the user's data centre. The user's data centre has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-123456. to allow traffic to the internet from the VPN subnet. Which of the below mentioned options is not a valid entry for the main route table in this scenario?

- A. Destination: 20.0.1.0/24 and Target: i-12345
- B. Destination: 0.0.0.0/0 and Target: i-12345
- C. Destination: 172.28.0.0/12 and Target: vgw-12345
- D. Destination: 20.0.0.0/16 and Target: local

Answer: A

Explanation:

The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. When the user has configured this setup with Wizard, it will create a virtual private gateway to route all traffic of the VPN subnet. If the user has setup a NAT instance to route all the internet requests then all requests to the internet should be routed to it. All requests to the organization's DC will be routed to the VPN gateway. Here are the valid entries for the main route table in this scenario:
Destination: 0.0.0.0/0 & Target: i-12345 (To route all internet traffic to the NAT Instance. Destination: 172.28.0.0/12 & Target: vgw-12345 (To route all the organization's data centre traffic to the VPN gateway. Destination: 20.0.0.0/16 & Target: local (To allow local routing in VPC.

NEW QUESTION 329

- (Topic 3)

A user has enabled termination protection on an EC2 instance. The user has also set Instance initiated shutdown behaviour to terminate. When the user shuts down the instance from the OS, what will happen?

- A. The OS will shutdown but the instance will not be terminated due to protection
- B. It will terminate the instance
- C. It will not allow the user to shutdown the instance from the OS
- D. It is not possible to set the termination protection when an Instance initiated shutdown is set to Terminate

Answer: B

Explanation:

It is always possible that someone can terminate an EC2 instance using the Amazon EC2 console, command line interface or API by mistake. If the admin wants to prevent the instance from being accidentally terminated, he can enable termination protection for that instance. The user can also setup shutdown behaviour for an EBS backed instance to guide the instance on what should be done when he initiates shutdown from the OS using Instance initiated shutdown behaviour. If the instance initiated behaviour is set to terminate and the user shuts off the OS even though termination protection is enabled, it will still terminate the instance.

NEW QUESTION 334

- (Topic 3)

An organization is measuring the latency of an application every minute and storing data inside a file in the JSON format. The organization wants to send all latency data to AWS CloudWatch. How can the organization achieve this?

- A. The user has to parse the file before uploading data to CloudWatch

- B. It is not possible to upload the custom data to CloudWatch
- C. The user can supply the file as an input to the CloudWatch command
- D. The user can use the CloudWatch Import command to import data from the file to CloudWatch

Answer: C

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user has to always include the namespace as part of the request. If the user wants to upload the custom data from a Amazon AWS-SysOps : Practice Test file, he can supply file name along with the parameter -- metric-data to command put-metric-data.

NEW QUESTION 335

- (Topic 3)

A user has created an Auto Scaling group using CLI. The user wants to enable CloudWatch detailed monitoring for that group. How can the user configure this?

- A. When the user sets an alarm on the Auto Scaling group, it automatically enables detail monitoring
- B. By default detailed monitoring is enabled for Auto Scaling
- C. Auto Scaling does not support detailed monitoring
- D. Enable detail monitoring from the AWS console

Answer: B

Explanation:

CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates an Auto Scaling launch config as the first step for creating an Auto Scaling group, each launch configuration contains a flag named InstanceMonitoring.Enabled. The default value of this flag is true. Thus, the user does not need to set this flag if he wants detailed monitoring.

NEW QUESTION 338

- (Topic 3)

A user has granted read/write permission of his S3 bucket using ACL. Which of the below mentioned options is a valid ID to grant permission to other AWS accounts (grantee) using ACL?

- A. IAM User ID
- B. S3 Secure ID
- C. Access ID
- D. Canonical user ID

Answer: D

Explanation:

An S3 bucket ACL grantee can be an AWS account or one of the predefined Amazon S3 groups. The user can grant permission to an AWS account by the email address of that account or by the canonical user ID. If the user provides an email in the grant request, Amazon S3 finds the canonical user ID for that account and adds it to the ACL. The resulting ACL will always contain the canonical user ID for the AWS account, and not the AWS account's email address.

NEW QUESTION 343

- (Topic 3)

A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 by mistake. The user is trying to create another subnet of CIDR 20.0.0.1/24. How can the user create the second subnet?

- A. There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet's CIDR
- B. The user can modify the first subnet CIDR from the console
- C. It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been created
- D. The user can modify the first subnet CIDR with AWS CLI

Answer: D

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside the subnet. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet. The user cannot modify the CIDR of a subnet once it is created. Thus, in this case if required, the user has to delete the subnet and create new subnets.

NEW QUESTION 347

- (Topic 3)

A user has launched a Windows based EC2 instance. However, the instance has some issues and the user wants to check the log. When the user checks the Instance console output from the AWS console, what will it display?

- A. All the event logs since instance boot
- B. The last 10 system event log error
- C. The Windows instance does not support the console output
- D. The last three system events' log errors

Answer: D

Explanation:

The AWS EC2 console provides a useful tool called Console output for problem diagnosis. It is useful to find out any kernel issues, termination reasons or service configuration issues. For a Windows instance it lists the last three system event log errors. For Linux it displays the exact console output.

NEW QUESTION 351

- (Topic 3)

Your organization is preparing for a security assessment of your use of AWS.

In preparation for this assessment, which two IAM best practices should you consider implementing? Choose 2 answers

- A. Create individual IAM users for everyone in your organization
- B. Configure MFA on the root account and for privileged IAM users
- C. Assign IAM users and groups configured with policies granting least privilege access
- D. Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate

Answer: BC

Explanation:

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

NEW QUESTION 353

- (Topic 3)

A user has created a VPC with CIDR 20.0.0.0/16 using VPC Wizard. The user has created a public CIDR

(20.0.0.0/24. and a VPN only subnet CIDR (20.0.1.0/24. along with the hardware VPN access to connect to the user's data centre. Which of the below mentioned components is not present when the VPC is setup with the wizard?

- A. Main route table attached with a VPN only subnet
- B. A NAT instance configured to allow the VPN subnet instances to connect with the internet
- C. Custom route table attached with a public subnet
- D. An internet gateway for a public subnet

Answer: B

Explanation:

The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. When the user has configured this setup with Wizard, it will update the main route table used with the VPN-only subnet, create a custom route table and associate it with the public subnet. It also creates an internet gateway for the public subnet. The wizard does not create a NAT instance by default. The user can create it manually and attach it with a VPN only subnet.

NEW QUESTION 358

.....

Relate Links

100% Pass Your AWS-SysOps Exam with ExamBible Prep Materials

<https://www.exambible.com/AWS-SysOps-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>

1) Why is AWS more economical than traditional data centers for applications with varying compute workloads?

- A) Amazon EC2 costs are billed on a monthly basis.
- B) Users retain full administrative access to their Amazon EC2 instances.
- C) Amazon EC2 instances can be launched on demand when needed.
- D) Users can permanently run enough instances to handle peak workloads.

2) Which AWS service would simplify the migration of a database to AWS?

- A) AWS Storage Gateway
- B) AWS Database Migration Service (AWS DMS)
- C) Amazon EC2
- D) Amazon AppStream 2.0

3) Which AWS offering enables users to find, buy, and immediately start using software solutions in their AWS environment?

- A) AWS Config
- B) AWS OpsWorks
- C) AWS SDK
- D) AWS Marketplace

4) Which AWS networking service enables a company to create a virtual network within AWS?

- A) AWS Config
- B) Amazon Route 53
- C) AWS Direct Connect
- D) Amazon Virtual Private Cloud (Amazon VPC)

5) Which of the following is an AWS responsibility under the AWS shared responsibility model?

- A) Configuring third-party applications
- B) Maintaining physical hardware
- C) Securing application access and data
- D) Managing guest operating systems

6) Which component of the AWS global infrastructure does Amazon CloudFront use to ensure low-latency delivery?

- A) AWS Regions
- B) Edge locations
- C) Availability Zones
- D) Virtual Private Cloud (VPC)

7) How would a system administrator add an additional layer of login security to a user's AWS Management Console?

- A) Use Amazon Cloud Directory
- B) Audit AWS Identity and Access Management (IAM) roles
- C) Enable multi-factor authentication
- D) Enable AWS CloudTrail

8) Which service can identify the user that made the API call when an Amazon EC2 instance is terminated?

- A) AWS Trusted Advisor
- B) AWS CloudTrail
- C) AWS X-Ray
- D) AWS Identity and Access Management (AWS IAM)

9) Which service would be used to send alerts based on Amazon CloudWatch alarms?

- A) Amazon Simple Notification Service (Amazon SNS)
- B) AWS CloudTrail
- C) AWS Trusted Advisor
- D) Amazon Route 53

10) Where can a user find information about prohibited actions on the AWS infrastructure?

- A) AWS Trusted Advisor
- B) AWS Identity and Access Management (IAM)
- C) AWS Billing Console
- D) AWS Acceptable Use Policy

Answers

- 1) C – The ability to [launch instances on demand](#) when needed allows users to launch and terminate instances in response to a varying workload. This is a more economical practice than purchasing enough on-premises servers to handle the peak load.
- 2) B – AWS DMS helps users migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. [AWS DMS](#) can migrate data to and from most widely used commercial and open-source databases.
- 3) D – [AWS Marketplace](#) is a digital catalog with thousands of software listings from independent software vendors that makes it easy to find, test, buy, and deploy software that runs on AWS.
- 4) D – [Amazon VPC](#) lets users provision a logically isolated section of the AWS Cloud where users can launch AWS resources in a virtual network that they define.
- 5) B – Maintaining physical hardware is an AWS responsibility under the [AWS shared responsibility model](#).
- 6) B – To deliver content to users with lower latency, [Amazon CloudFront](#) uses a global network of points of presence (edge locations and regional edge caches) worldwide.
- 7) C – [Multi-factor authentication](#) (MFA) is a simple best practice that adds an extra layer of protection on top of a username and password. With MFA enabled, when a user signs in to an AWS Management Console, they will be prompted for their username and password (the first factor—what they know), as well as for an authentication code from their MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for AWS account settings and resources.
- 8) B – [AWS CloudTrail](#) helps users enable governance, compliance, and operational and risk auditing of their AWS accounts. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs.
- 9) A – Amazon SNS and Amazon CloudWatch are integrated so users can collect, view, and analyze metrics for every active SNS. Once users have configured [CloudWatch for Amazon SNS](#), they can gain better insight into the performance of their Amazon SNS topics, push notifications, and SMS deliveries.
- 10) D – The [AWS Acceptable Use Policy](#) provides information regarding prohibited actions on the AWS infrastructure.

1) A company is migrating a legacy web application from a single server to multiple Amazon EC2 instances behind an Application Load Balancer (ALB). After the migration, users report that they are frequently losing their sessions and are being prompted to log in again.

Which action should be taken to resolve the issue reported by users?

- A) Confirm that the ALB is not in a multi-AZ configuration.
- B) Configure an Amazon CloudFront distribution with the ALB as the origin.
- C) Deploy a Network Load Balancer in front of the ALB.
- D) Enable sticky sessions for the target group of EC2 instances.

2) A SysOps team checks their AWS Personal Health Dashboard every week for upcoming AWS hardware maintenance events. Recently, a team member was on vacation and the team missed an event, which resulted in an outage. The team wants a simple method to ensure that everyone is aware of upcoming events without depending on an individual team member checking the dashboard.

What should be done to address this?

- A) Build a web scraper to monitor the Personal Health Dashboard. When new health events are detected, send a notification to an Amazon SNS topic monitored by the entire team.
- B) Create an Amazon CloudWatch Events event based off the AWS Health service and send a notification to an Amazon SNS topic monitored by the entire team.
- C) Create an Amazon CloudWatch Events event that sends a notification to an Amazon SNS topic monitored by the entire team to remind the team to view the maintenance events on the Personal Health Dashboard.
- D) Create an AWS Lambda function that continuously pings all EC2 instances to confirm their health. Alert the team if this check fails.

3) An application running in a VPC needs to access instances owned by a different account and running in a VPC in a different Region. For compliance purposes, the traffic must not traverse the public internet.

How should an Administrator configure network routing to meet these requirements?

- A) Within each account, create a custom routing table containing routes that point to the other account's virtual private gateway.
- B) Within each account, set up a NAT gateway in a public subnet in its respective VPC. Then, using the public IP address from the NAT gateway, enable routing between the two VPCs.
- C) From one account, configure a Site-to-Site VPN connection between the VPCs. Within each account, add routes in the VPC route tables that point to the CIDR block of the remote VPC.
- D) From one account, create a VPC peering request. After an Administrator from the other account accepts the request, add routes in the route tables for each VPC that point to the CIDR block of the peered VPC.

4) An application running on Amazon EC2 instances needs to access data stored in an Amazon DynamoDB table.

Which solution will grant the application access to the table in the MOST secure manner?

- A) Create an IAM group for the application and attach a permissions policy with the necessary privileges. Add the EC2 instances to the IAM group.

AWS Certified SysOps Administrator–Associate (SOA-C01) Sample Exam Questions

- B) Create an IAM resource policy for the DynamoDB table that grants the necessary permissions to Amazon EC2.
- C) Create an IAM role with the necessary privileges to access the DynamoDB table. Associate the role with the EC2 instances.
- D) Create an IAM user for the application and attach a permissions policy with the necessary privileges. Generate an access key and embed the key in the application code.

5) A third-party service uploads objects to Amazon S3 every night. Occasionally, the service uploads an incorrectly formatted version of an object. In these cases, the SysOps Administrator needs to recover an older version of the object.

What is the MOST efficient way to recover the object without having to retrieve it from the remote service?

- A) Configure an Amazon CloudWatch Events scheduled event that triggers an AWS Lambda function that backs up the S3 bucket prior to the nightly job. When bad objects are discovered, restore the backed up version.
- B) Create an S3 event on object creation that copies the object to an Amazon Elasticsearch Service (Amazon ES) cluster. When bad objects are discovered, retrieve the previous version from Amazon ES.
- C) Create an AWS Lambda function that copies the object to an S3 bucket owned by a different account. Trigger the function when new objects are created in S3. When bad objects are discovered, retrieve the previous version from the other account.
- D) Enable versioning on the S3 bucket. When bad objects are discovered, access previous versions with the CLI or AWS Management Console.

6) According to the AWS shared responsibility model, for which of the following Amazon EC2 activities is AWS responsible? (Select TWO.)

- A) Configuring network ACLs
- B) Maintaining network infrastructure
- C) Monitoring memory utilization
- D) Patching the guest operating system
- E) Patching the hypervisor

7) A Security and Compliance team requires that all Amazon EC2 workloads use approved Amazon Machine Images (AMIs). A SysOps Administrator must implement a process to find EC2 instances launched from unapproved AMIs.

Which solution will meet these requirements?

- A) Create a custom report using AWS Systems Manager inventory to identify unapproved AMIs.
- B) Run Amazon Inspector on each EC2 instance and flag the instance if it is using unapproved AMIs.
- C) Use an AWS Config rule to identify unapproved AMIs.
- D) Use AWS Trusted Advisor to identify the EC2 workloads using unapproved AMIs.

8) A SysOps Administrator observes a large number of rogue HTTP requests on an Application Load Balancer. The requests originate from various IP addresses. These requests cause increased server load and costs.

What should the SysOps Administrator do to block this traffic?

- A) Install Amazon Inspector on Amazon EC2 instances to block the traffic.
- B) Use Amazon GuardDuty to protect the web servers from bots and scrapers.
- C) Use AWS Lambda to analyze the web server logs, detect bot traffic, and block the IP addresses in the security groups.
- D) Use AWS WAF rate-based blacklisting to block the traffic when it exceeds a threshold.

9) A SysOps Administrator is implementing security group policies for a web application running on AWS. An Elastic Load Balancer connects to a fleet of Amazon EC2 instances that connect to an Amazon RDS database over port 1521. The security groups are named elbSG, ec2SG, and rdsSG, respectively.

How should these security groups be implemented?

- A) elbSG: allow port 80 and 443 from 0.0.0.0/0;
ec2SG: allow port 443 from elbSG;
rdsSG: allow port 1521 from ec2SG.
- B) elbSG: allow port 80 and 443 from 0.0.0.0/0;
ec2SG: allow port 80 and 443 from elbSG and rdsSG;
rdsSG: allow port 1521 from ec2SG.
- C) elbSG: allow port 80 and 443 from ec2SG;
ec2SG: allow port 80 and 443 from elbSG and rdsSG;
rdsSG: allow port 1521 from ec2SG.
- D) elbSG: allow port 80 and 443 from ec2SG;
ec2SG: allow port 443 from elbSG;
rdsSG: allow port 1521 from elbSG.

10) An ecommerce company wants to lower costs on its nightly jobs that aggregate the current day's sales and store the results in Amazon S3. The jobs run on multiple on-demand instances, and the jobs take just under 2 hours to complete. The jobs can run at any time during the night. If the job fails for any reason, it needs to be started from the beginning.

Which solution is the MOST cost-effective based on these requirements?

- A) Purchase Reserved Instances.
- B) Submit a request for a Spot block.
- C) Submit a request for all Spot Instances.
- D) Use a mixture of On-Demand and Spot Instances.

Answers

- 1) D – Legacy applications designed to run on a single server frequently store session data locally. When these applications are deployed on multiple instances behind a load balancer, user requests are routed to instances using the round robin routing algorithm. Session data stored on one instance would not be present on the others. By enabling [sticky sessions](#), cookies are used to track user requests and keep subsequent requests going to the same instance.
- 2) B – The AWS Health service publishes [Amazon CloudWatch Events](#). CloudWatch Events can trigger Amazon SNS notifications. This method requires neither additional coding nor infrastructure. It automatically notifies the team of upcoming events, and does not depend upon brittle solutions like web scraping.
- 3) D – A [VPC peering connection](#) enables routing using each VPC's private IP addresses as if they were in the same network. Traffic using inter-Region VPC peering always stays on the global AWS backbone and never traverses the public internet.
- 4) C - An [IAM role](#) can be used to provide permissions for applications that are running on Amazon EC2 instances to make AWS API requests using temporary credentials.
- 5) D – Enabling [versioning](#) is a simple solution. (A) involves writing custom code, (C) has no versioning, so the replication will overwrite the old version with the bad version if the error is not discovered quickly, and (B) will involve expensive storage that is not well suited for objects.
- 6) B, E – AWS provides [security of the cloud](#), including maintenance of the hardware and hypervisor software supporting Amazon EC2. Customers are responsible for any maintenance or monitoring within an EC2 instance, and for configuring their VPC infrastructure.
- 7) C – AWS Config has a [managed rule](#) that handles this scenario.
- 8) D – AWS WAF has rules that can protect web applications from [HTTP flood](#) attacks.
- 9) A – elbSG must allow all web traffic (HTTP and HTTPS) from the internet. ec2SG must allow traffic only from the load balancer only, in this case identified as traffic from elbSG. The database must allow traffic from the EC2 instances only, in this case identified as traffic from ec2SG.
- 10) B – The solution will take advantage of Spot pricing, but by using a [Spot block](#) instead of Spot Instances, the company can be assured the job will not be interrupted.



Amazon

Exam Questions AWS-SysOps

AWS Certified SysOps Administrator - Associate (SOA-C01)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Topic 1)

When assessing an organization's use of AWS API access credentials which of the following three credentials should be evaluated?

Choose 3 answers

- A. Key pairs
- B. Console passwords
- C. Access keys
- D. Signing certificates
- E. Security Group memberships

Answer: ACD

Explanation:

Reference:

http://media.amazonwebservices.com/AWS_Operational_Checklists.pdf

NEW QUESTION 2

- (Topic 1)

You are creating an Auto Scaling group whose Instances need to insert a custom metric into CloudWatch.

Which method would be the best way to authenticate your CloudWatch PUT request?

- A. Create an IAM role with the Put MetricData permission and modify the Auto Scaling launch configuration to launch instances in that role
- B. Create an IAM user with the PutMetricData permission and modify the Auto Scaling launch configuration to inject the user's credentials into the instance User Data
- C. Modify the appropriate Cloud Watch metric policies to allow the Put MetricData permission to instances from the Auto Scaling group
- D. Create an IAM user with the PutMetricData permission and put the credentials in a private repository and have applications on the server pull the credentials as needed

Answer: A

NEW QUESTION 3

- (Topic 2)

A user has created an ELB with the availability zone US-East-1A. The user wants to add more zones to ELB to achieve High Availability. How can the user add more zones to the existing ELB?

- A. It is not possible to add more zones to the existing ELB
- B. The only option is to launch instances in different zones and add to ELB
- C. The user should stop the ELB and add zones and instances as required
- D. The user can add zones on the fly from the AWS console

Answer: D

Explanation:

The user has created an Elastic Load Balancer with the availability zone and wants to add more zones to the existing ELB. The user can do so in two ways:

From the console or CLI, add new zones to ELB;

Launch instances in a separate AZ and add instances to the existing ELB.

NEW QUESTION 4

- (Topic 2)

A user is publishing custom metrics to CloudWatch. Which of the below mentioned statements will help the user understand the functionality better?

- A. The user can use the CloudWatch Import tool
- B. The user should be able to see the data in the console after around 15 minutes
- C. If the user is uploading the custom data, the user must supply the namespace, timezone, and metric name as part of the command
- D. The user can view as well as upload data using the console, CLI and APIs

Answer: B

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user has to always include the namespace as a part of the request. However, the other parameters are optional. If the user has uploaded data using CLI, he can view it as a graph inside the console. The data will take around 2 minutes to upload but can be viewed only after around 15 minutes.

NEW QUESTION 5

- (Topic 3)

A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the user should first understand the namespace for the AWS services. Which of the below mentioned is not a valid namespace for the AWS services?

- A. AWS/StorageGateway
- B. AWS/CloudTrail
- C. AWS/ElastiCache
- D. AWS/SWF

Answer: B

Explanation:

Amazon CloudWatch is basically a metrics repository. The AWS product puts metrics into this repository, and the user can retrieve the data or statistics based on those metrics. To distinguish the data for each service, the CloudWatch metric has a namespace. Namespaces are containers for metrics. All AWS services that provide the Amazon CloudWatch data use a namespace string, beginning with "AWS/". All the services which are supported by CloudWatch will have some namespace. CloudWatch does not monitor CloudTrail. Thus, the namespace "AWS/CloudTrail" is incorrect.

NEW QUESTION 6

- (Topic 3)

A sys admin has enabled logging on ELB. Which of the below mentioned fields will not be a part of the log file name?

- A. Load Balancer IP
- B. EC2 instance IP
- C. S3 bucket name
- D. Random string

Answer: B

Explanation:

Elastic Load Balancing access logs capture detailed information for all the requests made to the load balancer. Elastic Load Balancing publishes a log file from each load balancer node at the interval that the user has specified. The load balancer can deliver multiple logs for the same period. Elastic Load Balancing creates log file names in the following format: "{Bucket}/{Prefix}/AWSLogs/{AWS AccountID}/elasticloadbalancing/{Region}/{Year}/{Month}/{Day}/{AWS Account ID}_elasticloadbalancing_{Region}_{Load Balancer Name}_{End Time}_{Load Balancer IP}_{Random String}.log"

NEW QUESTION 7

- (Topic 3)

A user has launched 5 instances in EC2-CLASSIC and attached 5 elastic IPs to the five different instances in the US East region. The user is creating a VPC in the same region. The user wants to assign an elastic IP to the VPC instance. How can the user achieve this?

- A. The user has to request AWS to increase the number of elastic IPs associated with the account
- B. AWS allows 10 EC2 Classic IPs per region; so it will allow to allocate new Elastic IPs to the same region
- C. The AWS will not allow to create a new elastic IP in VPC; it will throw an error
- D. The user can allocate a new IP address in VPC as it has a different limit than EC2

Answer: D

Explanation:

Section: (none)

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. A user can have 5 IP addresses per region with EC2 Classic. The user can have 5 separate IPs with VPC in the same region as it has a separate limit than EC2 Classic.

NEW QUESTION 8

- (Topic 3)

When an EC2 instance that is backed by an S3-based AMI is terminated, what happens to the data on the root volume?

- A. Data is automatically deleted
- B. Data is automatically saved as an EBS snapshot
- C. Data is unavailable until the instance is restarted
- D. Data is automatically saved as an EBS volume

Answer: A

NEW QUESTION 9

- (Topic 3)

A user is having data generated randomly based on a certain event. The user wants to upload that data to CloudWatch. It may happen that event may not have data generated for some period due to randomness. Which of the below mentioned options is a recommended option for this case?

- A. For the period when there is no data, the user should not send the data at all
- B. For the period when there is no data the user should send a blank value
- C. For the period when there is no data the user should send the value as 0
- D. The user must upload the data to CloudWatch as having no data for some period will cause an error at CloudWatch monitoring

Answer: C

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. When the user data is more random and not generated at regular intervals, there can be a period which has no associated data. The user can either publish the zero (0) value for that period or not publish the data at all. It is recommended that the user should publish zero instead of no value to monitor the health of the application. This is helpful in an alarm as well as in the generation of the sample data count.

NEW QUESTION 10

- (Topic 3)

How can an EBS volume that is currently attached to an EC2 instance be migrated from one Availability Zone to another?

- A. Simply create a new volume in the other AZ and specify the original volume as the source

- B. Detach the volume, then use the ec2-migrate-volume command to move it to another A
- C. Create a snapshot of the volume, and create a new volume from the snapshot in the other A
- D. Detach the volume and attach it to another EC2 instance in the other A

Answer: D

Explanation:

Reference:
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html>

NEW QUESTION 11

- (Topic 3)

A root account owner has given full access of his S3 bucket to one of the IAM users using the bucket ACL. When the IAM user logs in to the S3 console, which actions can he perform?

- A. He can just view the content of the bucket
- B. He can do all the operations on the bucket
- C. It is not possible to give access to an IAM user using ACL
- D. The IAM user can perform all operations on the bucket using only API/SDK

Answer: C

Explanation:

Each AWS S3 bucket and object has an ACL (Access Control List) associated with it. An ACL is a list of grants identifying the grantee and the permission granted. The user can use ACLs to grant basic read/write permissions to other AWS accounts. ACLs use an Amazon S3-specific XML schema. The user cannot grant permissions to other users (IAM users) in his account.

NEW QUESTION 12

- (Topic 3)

You have private video content in S3 that you want to serve to subscribed users on the Internet. User IDs, credentials, and subscriptions are stored in an Amazon RDS database.

Which configuration will allow you to securely serve private content to your users?

- A. Generate pre-signed URLs for each user as they request access to protected S3 content
- B. Create an IAM user for each subscribed user and assign the GetObject permission to each IAM user
- C. Create an S3 bucket policy that limits access to your private content to only your subscribed users' credentials
- D. Create a CloudFront Origin Identity user for your subscribed users and assign the GetObject permission to this user

Answer: C

Explanation:

Reference:
<https://java.awsblog.com/post/Tx1VE22EWFR4H86/Accessing-Private-Content-in-Amazon-CloudFront>

NEW QUESTION 13

- (Topic 3)

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below mentioned entries is required in the web server security group (WebSecGrp)?

- A. Configure Destination as DB Security group ID (DbSecGr)
- B. for port 3306 Outbound
- C. 80 for Destination 0.0.0.0/0 Outbound
- D. Configure port 3306 for source 20.0.0.0/24 InBound
- E. Configure port 80 InBound for source 20.0.0.0/16

Answer: A

Explanation:

A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet to host the web server and DB server respectively, the user should configure that the instances in the public subnet can receive inbound traffic directly from the internet. Thus, the user should configure port 80 with source 0.0.0.0/0 in InBound. The user should configure that the instance in the public subnet can send traffic to the private subnet instances on the DB port. Thus, the user should configure the DB Amazon AWS-SysOps : Practice Test security group of the private subnet (DbSecGrp) as the destination for port 3306 in Outbound.

NEW QUESTION 14

- (Topic 3)

A user had aggregated the CloudWatch metric data on the AMI ID. The user observed some abnormal behaviour of the CPU utilization metric while viewing the last 2 weeks of data. The user wants to share that data with his manager. How can the user achieve this easily with the AWS console?

- A. The user can use the copy URL functionality of CloudWatch to share the exact details
- B. The user can use the export data option from the CloudWatch console to export the current data point
- C. The user has to find the period and data and provide all the aggregation information to the manager
- D. The user can use the CloudWatch data copy functionality to copy the current data points

Answer: A

Explanation:

Amazon CloudWatch provides the functionality to graph the metric data generated either by the AWS services or the custom metric to make it easier for the user to analyse. The console provides the option to save the URL or bookmark it so that it can be used in the future by typing the same URL. The Copy URL functionality is available under the console when the user selects any metric to view.

NEW QUESTION 15

- (Topic 3)

A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is not true in this scenario?

- A. The VPC will create a routing instance and attach it with a public subnet
- B. The VPC will create two subnets
- C. The VPC will create one internet gateway and attach it to VPC
- D. The VPC will launch one NAT instance with an elastic IP

Answer: A

Explanation:

A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance with an elastic IP. Wizard will also create two subnets with route tables. It will also create an internet gateway and attach it to the VPC.

NEW QUESTION 16

- (Topic 3)

A user is receiving a notification from the RDS DB whenever there is a change in the DB security group. The user does not want to receive these notifications for only a month. Thus, he does not want to delete the notification. How can the user configure this?

- A. Change the Disable button for notification to "Yes" in the RDS console
- B. Set the send mail flag to false in the DB event notification console
- C. The only option is to delete the notification from the console
- D. Change the Enable button for notification to "No" in the RDS console

Answer: D

Explanation:

Amazon RDS uses the Amazon Simple Notification Service to provide a notification when an Amazon RDS event occurs. Event notifications are sent to the addresses that the user has provided while creating the subscription. The user can easily turn off the notification without deleting a subscription by setting the Enabled radio button to No in the Amazon RDS console or by setting the Enabled parameter to false using the CLI or Amazon RDS API.

NEW QUESTION 17

- (Topic 3)

An organization is trying to create various IAM users. Which of the below mentioned options is not a valid IAM username?

- A. John.cloud
- B. john@cloud
- C. John=cloud
- D. john#cloud

Answer: D

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. Whenever the organization is creating an IAM user, there should be a unique ID for each user. The names of users, groups, roles, instance profiles must be alphanumeric, including the following common characters: plus (+), equal (=), comma (,), period (..), at (@..), and dash (-..).

NEW QUESTION 18

- (Topic 3)

A user has configured an SSL listener at ELB as well as on the back-end instances. Which of the below mentioned statements helps the user understand ELB traffic handling with respect to the SSL listener?

- A. It is not possible to have the SSL listener both at ELB and back-end instances
- B. ELB will modify headers to add requestor details
- C. ELB will intercept the request to add the cookie details if sticky session is enabled
- D. ELB will not modify the headers

Answer: D

Explanation:

When the user has configured Transmission Control Protocol (TCP) or Secure Sockets Layer (SSL) for both front-end and back-end connections of the Elastic Load Balancer, the load balancer forwards the request to the back-end instances without modifying the request headers unless the proxy header is enabled. SSL does not support sticky sessions. If the user has enabled a proxy protocol it adds the source and destination IP to the header.

NEW QUESTION 19

- (Topic 3)

A user is using a small MySQL RDS DB. The user is experiencing high latency due to the Multi AZ feature. Which of the below mentioned options may not help the user in this situation?

- A. Schedule the automated back up in non-working hours
- B. Use a large or higher size instance
- C. Use PIOPS
- D. Take a snapshot from standby Replica

Answer: D

Explanation:

An RDS DB instance which has enabled Multi AZ deployments may experience increased write and commit latency compared to a Single AZ deployment, due to synchronous data replication. The user may also face changes in latency if deployment fails over to the standby replica. For production workloads, AWS recommends the user to use provisioned IOPS and DB instance classes (m1.large and larger) as they are optimized for provisioned IOPS to give a fast, and consistent performance. With Multi AZ feature, the user can not have option to take snapshot from replica.

NEW QUESTION 20

- (Topic 3)

A user has launched an EBS backed instance with EC2-Classic. The user stops and starts the instance. Which of the below mentioned statements is not true with respect to the stop/start action?

- A. The instance gets new private and public IP addresses
- B. The volume is preserved
- C. The Elastic IP remains associated with the instance
- D. The instance may run on a anew host computer

Answer: C

Explanation:

A user can always stop/start an EBS backed EC2 instance. When the user stops the instance, it first enters the stopping state, and then the stopped state. AWS does not charge the running cost but charges only for the EBS storage cost. If the instance is running in EC2-Classic, it receives a new private IP address; as the Elastic IP address (EIP) associated with the instance is no longer associated with that instance.

NEW QUESTION 21

.....

Relate Links

100% Pass Your AWS-SysOps Exam with ExamBible Prep Materials

<https://www.exambible.com/AWS-SysOps-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>

IT Exam Certified

We help to get you certified in Cloud Technologies Oracle, AWS, Azure, GCP and all other IT exams

DVA-C01 AWS Certified Developer Associate

478.

A serverless application stores objects in an Amazon S3 bucket. S3 event notifications are configured for the bucket to invoke an AWS Lambda function each time a new object is created. The Lambda function has an IAM role that is assigned.

A developer discovers that the Lambda function is not invoked when a new object is stored in the S3 bucket.

What should the developer do so that the S3 event notifications will invoke the Lambda function?

- A. Grant the s3:GetObject permission with an Allow action type to the IAM role.
- B. Enable public access for the S3 bucket.
- C. Enable static website hosting for the S3 bucket.
- D. Grant permission to Amazon S3 to use the Lambda function.

Ans : D

479.

A developer is working on a serverless application. The application uses Amazon API Gateway, AWS Lambda functions that are written in Python, and Amazon DynamoDB.

Which combination of steps should the developer take so that the Lambda functions can be debugged in the event of application failures? (Select TWO.)

- A. Configure an AWS CloudTrail trail to deliver log files to an Amazon S3 bucket.
- B. Ensure that the Lambda functions write log messages to stdout and stderr.
- C. Enable an AWS CloudTrail trail for the Lambda function.
- D. Ensure that the execution role for the Lambda function has access to write to Amazon CloudWatch Logs.
- E. Use the Amazon CloudWatch metric for Lambda errors to create a CloudWatch alarm.

Ans BC

480.

<https://itexamcertified.com>

A developer for a small startup company is designing a web application. The company's customer service representatives will use the web application to look up order information. The design must use an existing Amazon DynamoDB table. The table consists of items that store an order's details. The table uses order ID as the primary key.

The developer wants to implement the web application as single-page application (SPA) that prompts the user to enter an order ID. The web application then will make a REST request to query and display the order details. The design must be scalable to support several thousand lookups each day.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure the web application to send an HTTPS request that contains an order ID to an Application Load Balancer (ALB). Configure the ALB to invoke an AWS Lambda function to query the order from the DynamoDB table.
- B. Configure the web application to send an HTTPS request that contains an order ID to an Application Load Balancer (ALB). Configure the ALB to query the order from the DynamoDB table.
- C. Configure the web application to send an HTTPS request that contains an order ID to a REST API method in Amazon API Gateway. Configure the API method to query the order from the DynamoDB table.
- D. Configure the web application to send an HTTPS request that contains an order ID to a REST API method in Amazon API Gateway. Configure the API method to invoke an AWS Lambda function to query the order from the DynamoDB table.

Ans : A

481.

A developer is deploying an AWS Serverless Application Model (AWS SAM) application. The developer is using a linear deployment for AWS Lambda functions. The deployment is configured to deploy 10% every 10 minutes. However, after 10 minutes, the associated alarms indicate a failure in the deployment.

What is the result of the deployment after the failure?

- A. The deployment halts with 20% of the traffic routed to the new version and will roll back to the original version.
- B. The deployment halts with 10% of the traffic updated to the new version, but all traffic will be routed to the old version.
- C. The deployment halts with 20% of the traffic routed to the new version and 80% of the traffic routed to the old version.
- D. The deployment halts. The user is prompted to continue the deployment to the new version or to roll back to the old version.

Ans : C

482.

A company is using AWS CloudFormation templates to deploy AWS resources. The company needs to update one of its AWS CloudFormation stacks.

What can the company do to find out how the changes will impact the resources that are running?

- A. Investigate the change sets.
- B. Investigate the stack policies.
- C. Investigate the Metadata section.
- D. Investigate the Resources section.

Ans :D

483.

A developer is writing a web application that is deployed on Amazon EC2 instances behind an internet-facing Application Load Balancer (ALB). The developer must add an Amazon CloudFront distribution in front of the ALB. The developer also must ensure that customer data from outside the VPC is encrypted in transit.

Which combination of CloudFront configuration settings should the developer use to meet these requirements ? (Select TWO.)

- A. Restrict viewer access by using signed URLs.
- B. Set the Origin Protocol Policy setting to Match Viewer.
- C. Enable field-level encryption.
- D. Enable automatic object compression.
- E. Set the Viewer Protocol Policy setting to Redirect HTTP to HTTPS.

<https://itexamcertified.com>

<https://itexamcertified.com>

Ans : CD

Question #1

A Developer created a dashboard for an application using Amazon API Gateway, Amazon S3, AWS Lambda, and Amazon RDS. The Developer needs an authentication mechanism allowing a user to sign in and view the dashboard. It must be accessible from mobile applications, desktops, and tablets, and must remember user preferences across platforms.

Which AWS service should the Developer use to support this authentication scenario?

- A. AWS KMS
- B. Amazon Cognito
- C. AWS Directory Service
- D. Amazon IAM

Answer: B

Question #2

A Developer has created an S3 bucket s3://mycoolapp and has enabled server access logging that points to the folder s3://mycoolapp/logs. The

Developer moved 100 KB of Cascading Style Sheets (CSS) documents to the folder s3://mycoolapp/css, and then stopped work. When the developer came back a few days later, the bucket was 50 GB.

What is the MOST likely cause of this situation?

- A. The CSS files were not compressed and S3 versioning was enabled.
- B. S3 replication was enabled on the bucket.
- C. Logging into the same bucket caused exponential log growth.
- D. An S3 lifecycle policy has moved the entire CSS file to S3 Infrequent Access.

Answer: C

Question #3

A Developer is creating an Auto Scaling group whose instances need to publish a custom metric to Amazon CloudWatch.

Which method would be the MOST secure way to authenticate a CloudWatch PUT request?

- A. Create an IAM user with PutMetricData permission and put the user credentials in a private repository; have applications pull the credentials as needed.

<https://itexamcertified.com>

- B. Create an IAM user with PutMetricData permission, and modify the Auto Scaling launch configuration to inject the user credentials into the instance user data.
- C. Modify the CloudWatch metric policies to allow the PutMetricData permission to instances from the Auto Scaling group.
- D. Create an IAM role with PutMetricData permission and modify the Auto Scaling launching configuration to launch instances using that role.

Answer: D

Question #4

A Developer is working on an application that tracks hundreds of millions of product reviews in an Amazon DynamoDB table. The records include the data elements shown in the table:

Name	Type	Description
reviewID	Number	16 digit UUID
starRating	Number	Integer 1-5 of user rating
comment	String	User comment string
productID	Number	Product ID being reviewed

Which field, when used as the partition key, would result in the MOST consistent performance using DynamoDB?

- A. starRating
- B. reviewID
- C. comment
- D. productID

Answer: B

Question #5

A Developer has written a serverless application using multiple AWS services. The business logic is written as a Lambda function which has dependencies on third-party libraries. The Lambda function endpoints will be exposed using Amazon API Gateway. The Lambda function will write the information to Amazon

DynamoDB. The Developer is ready to deploy the application but must have the ability to rollback. How can this deployment be automated, based on these requirements?

- A. Deploy using Amazon Lambda API operations to create the Lambda function by providing a deployment package.
- B. Use an AWS CloudFormation template and use CloudFormation syntax to define the Lambda function resource in the template.

<https://itexamcertified.com>

C. Use syntax conforming to the Serverless Application Model in the AWS CloudFormation template to define the Lambda function resource.

D. Create a bash script which uses AWS CLI to package and deploy the application.

Answer: C

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/automating-deployment.html>

Question #6

What are the steps to using the AWS CLI to launch a templatized serverless application?

A. Use AWS CloudFormation get-template then CloudFormation execute-change-set.

B. Use AWS CloudFormation validate-template then CloudFormation create-change-set.

C. Use AWS CloudFormation package then CloudFormation deploy.

D. Use AWS CloudFormation create-stack then CloudFormation update-stack.

Answer: C

Reference:

<https://github.com/awslabs/aws-sam-cli>

Question #7

A Developer is creating a web application that requires authentication, but also needs to support guest access to provide users limited access without having to authenticate. What service can provide support for the application to allow guest access?

A. IAM temporary credentials using AWS STS.

B. Amazon Directory Service

C. Amazon Cognito with unauthenticated access enabled

D. IAM with SAML integration

Answer: C

Reference:

<https://aws.amazon.com/cognito/faqs/>

<https://itexamcertified.com>

Question #8

An application takes 40 seconds to process instructions received in an Amazon SQS message.

Assuming the SQS queue is configured with the default VisibilityTimeout value, what is the BEST way, upon receiving a message, to ensure that no other instances can retrieve a message that has already been processed or is currently being processed?

- A. Use the ChangeMessageVisibility API to increase the VisibilityTimeout, then use the DeleteMessage API to delete the message.
- B. Use the DeleteMessage API call to delete the message from the queue, then call DeleteQueue API to remove the queue.
- C. Use the ChangeMessageVisibility API to decrease the timeout value, then use the DeleteMessage API to delete the message.
- D. Use the DeleteMessageVisibility API to cancel the VisibilityTimeout, then use the DeleteMessage API to delete the message.

Answer: A

Question #9

A Developer has implemented a Lambda function that needs to add new customers to an RDS database that is expected to run hundreds of times per hour. The

Lambda function is configured to use 512MB of RAM and is based on the following pseudo code:

```
def lambda_handler(event, context):  
  
    db = database.connect()  
  
    db.statement('INSERT INTO Customers (CustomerName) VALUES  
(context.name)')  
  
    db.close()
```

After testing the Lambda function, the Developer notices that the Lambda execution time is much longer than expected. What should the Developer do to improve performance?

- A. Increase the amount of RAM allocated to the Lambda function, which will increase the number of threads the Lambda can use.
- B. Increase the size of the RDS database to allow for an increased number of database connections each hour.
- C. Move the database connection and close statement out of the handler. Place the connection in the global space.
- D. Replace RDS with Amazon DynamoDB to implement control over the number of writes per second.

<https://itexamcertified.com>

Answer: C

Question #10

A current architecture uses many Lambda functions invoking one another as a large state machine. The coordination of this state machine is legacy custom code that breaks easily.

Which AWS Service can help refactor and manage the state machine?

- A. AWS Data Pipeline
- B. AWS SNS with AWS SQS
- C. Amazon Elastic MapReduce
- D. AWS Step Functions D

Answer: D

Reference:

<https://docs.aws.amazon.com/step-functions/latest/dg/tutorial-creating-lambda-state-machine.html>

Question #11

A Developer is asked to implement a caching layer in front of Amazon RDS. Cached content is expensive to regenerate in case of service failure. Which implementation below would work while maintaining maximum uptime?

- A. Implement Amazon ElastiCache Redis in Cluster Mode
- B. Install Redis on an Amazon EC2 instance.
- C. Implement Amazon ElastiCache Memcached.
- D. Migrate the database to Amazon Redshift.

Answer: A

Reference:

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

Question #12

A current architecture uses many Lambda functions invoking one another as large state machine. The coordination of this state machine is legacy custom code that breaks easily.

<https://itexamcertified.com>

<https://itexamcertified.com>

Which AWS Service can help refactor and manage the state machine?

- A. AWS Data Pipeline
- B. AWS SNS with AWS SQS
- C. Amazon Elastic MapReduce
- D. AWS Step Functions

Answer: D

Question #13

A large e-commerce site is being designed to deliver static objects from Amazon S3. The Amazon S3 bucket will server more than 300 GET requests per second.

What should be done to optimize performance? (Select TWO.)

- A. Integrate Amazon CloudFront with Amazon S3.
- B. Enable Amazon S3 cross-region replication.
- C. Delete expired Amazon S3 server log files.
- D. Configure Amazon S3 lifecycle rules.
- E. Randomize Amazon S3 key name prefixes.

Answer: AE

Reference:

<http://jayendrapatil.com/aws-s3-best-practices/>

Question #14

A company is building a stock trading application that requires sub-millisecond latency in processing trading requests. Amazon DynamoDB is used to store all the trading data that is used to process each request. After load testing the application, the development team found that due to data retrieval times, the latency requirement is not satisfied. Because of sudden high spikes in the number of requests, DynamoDB read capacity has to be significantly over-provisioned to avoid throttling.

What steps should be taken to meet latency requirements and reduce the cost of running the application?

- A. Add Global Secondary Indexes for trading data.
- B. Store trading data in Amazon S3 and use Transfer Acceleration.
- C. Add retries with exponential back-off for DynamoDB queries

<https://itexamcertified.com>

<https://itexamcertified.com>

- D. Use DynamoDB Accelerator to cache trading data.

Answer: D

Question #15

A Developer needs temporary access to resources in a second account.

What is the MOST secure way to achieve this?

- A. Use the Amazon Cognito user pools to get short-lived credentials for the second account.
- B. Create a dedicated IAM access key for the second account, and send it by mail.
- C. Create a cross-account access role, and use sts:AssumeRole API to get short-lived credentials.
- D. Establish trust, and add an SSH key for the second account to the IAM user.

Answer: C

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

Question #16

An application reads data from an Amazon DynamoDB table. Several times a day, for a period of 15 seconds, the application receives multiple errors.

ProvisionedThroughputExceeded -

How should this exception be handled?

- A. Create a new global secondary index for the table to help with the additional requests.
- B. Retry the failed read requests with exponential backoff.
- C. Immediately retry the failed read requests.
- D. Use the DynamoDB "UpdateItem" API to increase the provisioned throughput capacity of the table.

Answer: B

Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-query-scan.html>

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #17

A Developer has created a large Lambda function, and deployment is failing with the following error:

ClientError: An error occurred (InvalidParameterValueException) when calling the CreateFunction operation: Unzipped size must be smaller than XXXXXXXXX bytes', where XXXXXXXXX is the current Lambda limit

What can the Developer do to fix this problem?

- A. Submit a limit increase request to AWS Support to increase the function to the size needed.
- B. Use a compression algorithm that is more efficient than ZIP.
- C. Break the function into multiple smaller Lambda functions.
- D. ZIP the ZIP file twice to compress it further.

Answer: C

Question #18

Given the source code for an AWS Lambda function in the local store.py containing a handler function called get_store and the following AWS

CloudFormation template:

Transform: AWS::Serverless-2016-10-31

Resources:

 StoreFunc:

 Type: AWS::Serverless::Function

 Properties:

 Handler: store.get_store

 Runtime: python3.6

What should be done to prepare the template so that it can be deployed using the AWS CLI command aws cloudformation deploy?

- A. Use aws cloudformation compile to base64 encode and embed the source file into a modified CloudFormation template.
- B. Use aws cloudformation package to upload the source code to an Amazon S3 bucket and produce a modified CloudFormation template.
- C. Use aws lambda zip to package the source file together with the CloudFormation template and deploy the resulting zip archive.

<https://itexamcertified.com>

<https://itexamcertified.com>

D. Use aws serverless create-package to embed the source file directly into the existing CloudFormation template.

Answer: B

Question #19

An application stores images in an S3 bucket. Amazon S3 event notifications are used to trigger a Lambda function that resizes the images. Processing each image takes less than a second.

How will AWS Lambda handle the additional traffic?

- A. Lambda will scale out to execute the requests concurrently.
- B. Lambda will handle the requests sequentially in the order received.
- C. Lambda will process multiple images in a single execution.
- D. Lambda will add more compute to each execution to reduce processing time.

Answer: A

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/scaling.html>

Question #20

A company wants to implement a continuous integration for its workloads on AWS. The company wants to trigger unit test in its pipeline for commits on its code repository, and wants to be notified of failure events in the pipeline.

How can these requirements be met?

- A. Store the source code in AWS CodeCommit. Create a CodePipeline to automate unit testing. Use Amazon SNS to trigger notifications of failure events.
- B. Store the source code in GitHub. Create a CodePipeline to automate unit testing. Use Amazon SES to trigger notifications of failure events.
- C. Store the source code on GitHub. Create a CodePipeline to automate unit testing. Use Amazon CloudWatch to trigger notifications of failure events.
- D. Store the source code in AWS CodeCommit. Create a CodePipeline to automate unit testing. Use Amazon CloudWatch to trigger notification of failure events.

Answer: D

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #21

A serverless application uses an API Gateway and AWS Lambda.

Where should the Lambda function store its session information across function calls?

- A. In an Amazon DynamoDB table
- B. In an Amazon SQS queue
- C. In the local filesystem
- D. In an SQLite session table using ""DSQLITE_ENABLE_SESSION A

Answer: A

Question #22

A Developer has created a software package to be deployed on multiple EC2 instances using IAM roles.

What actions could be performed to verify IAM access to get records from Amazon Kinesis Streams? (Select TWO.)

- A. Use the AWS CLI to retrieve the IAM group.
- B. Query Amazon EC2 metadata for in-line IAM policies.
- C. Request a token from AWS STS, and perform a describe action.
- D. Perform a get action using the ""-dry-run argument.
- E. Validate the IAM role policy with the IAM policy simulator.

Answer: BE

Question #23

When writing a Lambda function, what is the benefit of instantiating AWS clients outside the scope of the handler?

- A. Legibility and stylistic convention
- B. Taking advantage of connection re-use
- C. Better error handling
- D. Creating a new instance per invocation

Answer: B

Reference:

<https://www.jeremydaly.com/reuse-database-connections-aws-lambda/>

<https://itexamcertified.com>

Question #24

An application on AWS is using third-party APIs. The Developer needs to monitor API errors in the code, and wants to receive notifications if failures go above a set threshold value.

How can the Developer achieve these requirements?

- A. Publish a custom metric on Amazon CloudWatch and use Amazon SES for notification.
- B. Use an Amazon CloudWatch API-error metric and use Amazon SNS for notification.
- C. Use an Amazon CloudWatch API-error metric and use Amazon SES for notification.
- D. Publish a custom metric on Amazon CloudWatch and use Amazon SNS for notification.

Answer: D

Question #25

A Developer has an application that can upload tens of thousands of objects per second to Amazon S3 in parallel within a single AWS account. As part of new requirements, data stored in S3 must use server side encryption with AWS KMS (SSE-KMS). After creating this change, performance of the application is slower.

Which of the following is MOST likely the cause of the application latency?

- A. Amazon S3 throttles the rate at which uploaded objects can be encrypted using Customer Master Keys.
- B. The AWS KMS API calls limit is less than needed to achieve the desired performance.
- C. The client encryption of the objects is using a poor algorithm.
- D. KMS requires that an alias be used to create an independent display name that can be mapped to a CMK.

Answer: B

Question #26

A company wants to migrate its web application to AWS and leverage Auto Scaling to handle peak workloads. The Solutions Architect determined that the best metric for an Auto Scaling event is the number of concurrent users.

Based on this information, what should the Developer use to autoscale based on concurrent users?

- A. An Amazon SNS topic to be triggered when a concurrent user threshold is met
- B. An Amazon Cloudwatch Networkin metric
- C. Amazon CloudFront to leverage AWS Edge Locations
- D. A Custom Amazon CloudWatch metric for concurrent users. D

<https://itexamcertified.com>

Answer: D

Question #27

A company is migrating its on-premises database to Amazon RDS for MySQL. The company has read-heavy workloads, and wants to make sure it re-factors its code to achieve optimum read performance for its queries.

How can this objective be met?

- A. Add database retries to effectively use RDS with vertical scaling
- B. Use RDS with multi-AZ deployment
- C. Add a connection string to use an RDS read replica for read queries
- D. Add a connection string to use a read replica on an EC2 instance. C

Answer: C

Question #28

A Developer is receiving HTTP 400: ThrottlingException errors intermittently when calling the Amazon CloudWatch API. When a call fails, no data is retrieved.

What best practice should first be applied to address this issue?

- A. Contact AWS Support for a limit increase.
- B. Use the AWS CLI to get the metrics
- C. Analyze the applications and remove the API call
- D. Retry the call with exponential backoff

Answer: D

Question #29

A Developer is testing a Docker-based application that uses the AWS SDK to interact with Amazon DynamoDB. In the local development environment, the application has used IAM access keys. The application is now ready for deployment onto an ECS cluster.

How should the application authenticate with AWS services in production?

- A. Configure an ECS task IAM role for the application to use
- B. Refactor the application to call AWS STS AssumeRole based on an instance role

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. Configure AWS access key/secret access key environment variables with new credentials
- D. Configure the credentials file with a new access key/secret access key

Answer: A

Question #30

A Developer created a Lambda function for a web application backend. When testing the Lambda function from the AWS Lambda console, the Developer can see that the function is being executed, but there is no log data being generated in Amazon CloudWatch Logs, even after several minutes.

What could cause this situation?

- A. The Lambda function does not have any explicit log statements for the log data to send it to CloudWatch Logs.
- B. The Lambda function is missing CloudWatch Logs as a source trigger to send log data.
- C. The execution role for the Lambda function is missing permissions to write log data to the CloudWatch Logs.
- D. The Lambda function is missing a target CloudWatch Log group.

Answer: C

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions.html>

(see note)

Question #31

An application has hundreds of users. Each user may use multiple devices to access the application. The Developer wants to assign unique identifiers to these users regardless of the device they use.

Which of the following methods should be used to obtain unique identifiers?

- A. Create a user table in Amazon DynamoDB as key-value pairs of users and their devices. Use these keys as unique identifiers.
- B. Use IAM-generated access key IDs for the users as the unique identifier, but do not store secret keys.
- C. Implement developer-authenticated identities by using Amazon Cognito, and get credentials for these identities.
- D. Assign IAM users and roles to the users. Use the unique IAM resource ID as the unique identifier.

Answer: C

<https://itexamcertified.com>

Question #32

An application is designed to use Amazon SQS to manage messages from many independent senders. Each sender's messages must be processed in the order they are received.

Which SQS feature should be implemented by the Developer?

- A. Configure each sender with a unique MessageGroupId
- B. Enable MessageDeduplicationIds on the SQS queue
- C. Configure each message with unique MessageGroupIds.
- D. Enable ContentBasedDeduplication on the SQS queue

Answer: A

Reference:

<https://aws.amazon.com/blogs/developer/how-the-amazon-sqs-fifo-api-works/>

Question #33

A deployment package uses the AWS CLI to copy files into any S3 bucket in the account, using access keys stored in environment variables. The package is running on EC2 instances, and the instances have been modified to run with an assumed IAM role and a more restrictive policy that allows access to only one bucket. After the change, the Developer logs into the host and still has the ability to write into all of the S3 buckets in that account.

What is the MOST likely cause of this situation?

- A. An IAM inline policy is being used on the IAM role
- B. An IAM managed policy is being used on the IAM role
- C. The AWS CLI is corrupt and needs to be reinstalled
- D. The AWS credential provider looks for instance profile credentials last

Answer: D

Question #34

A Developer is writing transactions into a DynamoDB table called "SystemUpdates" that has 5 write capacity units.

Which option has the highest read throughput?

- A. Eventually consistent reads of 5 read capacity units reading items that are 4 KB in size
- B. Strongly consistent reads of 5 read capacity units reading items that are 4 KB in size

<https://itexamcertified.com>

- C. Eventually consistent reads of 15 read capacity units reading items that are 1 KB in size
- D. Strongly consistent reads of 15 read capacity units reading items that are 1 KB in size

Answer: A

Question #35

Where should an Elastic Beanstalk configuration file named healthcheckur1.config be placed in the application source bundle?

- A. In the root of the application
- B. In the bin folder
- C. In healthcheckur1.config.ebextension under root
- D. In the .ebextensions folder

Answer: D

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/ebextensions.html>

Question #36

During non-peak hours, a Developer wants to minimize the execution time of a full Amazon DynamoDB table scan without affecting normal workloads. The workloads average half of the strongly consistent read capacity units during non-peak hours.

How would the Developer optimize this scan?

- A. Use parallel scans while limiting the rate
- B. Use sequential scans
- C. Increase read capacity units during the scan operation
- D. Change consistency to eventually consistent during the scan operation B

Answer: A

Question #37

A Developer is creating a Lambda function and will be using external libraries that are not included in the standard Lambda libraries.

<https://itexamcertified.com>

<https://itexamcertified.com>

What action would minimize the Lambda compute time consumed?

- A. Install the dependencies and external libraries at the beginning of the Lambda function.
- B. Create a Lambda deployment package that includes the external libraries.
- C. Copy the external libraries to Amazon S3, and reference the external libraries to the S3 location.
- D. Install the external libraries in Lambda to be available to all Lambda functions.

Answer: B

Question #38

A Developer is writing a Linux-based application to run on AWS Elastic Beanstalk. Application requirements state that the application must maintain full capacity during updates while minimizing cost.

Which type of Elastic Beanstalk deployment policy should the Developer specify for the environment?

- A. Immutable
- B. Rolling
- C. All at Once
- D. Rolling with additional batch

Answer: D

Reference:

<https://aws.amazon.com/about-aws/whats-new/2016/04/aws-elastic-beanstalk-adds-two-new-deployment-policies-and-amazon-linux-ami-2016-03-update/>

Question #39

An application under development is required to store hundreds of video files. The data must be encrypted within the application prior to storage, with a unique key for each video file.

How should the Developer code the application?

- A. Use the KMS Encrypt API to encrypt the data. Store the encrypted data key and data.
- B. Use a cryptography library to generate an encryption key for the application. Use the encryption key to encrypt the data. Store the encrypted data.
- C. Use the KMS GenerateDataKey API to get a data key. Encrypt the data with the data key. Store the encrypted data key and data.
- D. Upload the data to an S3 bucket using server side-encryption with an AWS KMS key.

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: C

Question #40

A Developer is creating an application that needs to locate the public IPv4 address of the Amazon EC2 instance on which it runs. How can the application locate this information?

- A. Get the instance metadata by retrieving <http://169.254.169.254/latest/metadata/>.
- B. Get the instance user data by retrieving <http://169.254.169.254/latest/userdata/>.
- C. Get the application to run IFCONFIG to get the public IP address.
- D. Get the application to run IPCONFIG to get the public IP address.

Answer: A

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>

Question #41

The Lambda function below is being called through an API using Amazon API Gateway. The average execution time for the Lambda function is about 1 second.

<https://itexamcertified.com>

The pseudocode for the Lambda function is as shown in the exhibit.

```
include "3rd party encryption module"  
include "match module"  
lambda_ handler(event, context)  
    rds_host = "rds-instance-endpoint"  
    name = db_udername  
    password = db_password  
    db_name = db_name  
# Connect to the RDS Database  
Conn = RDSCconnection(rds_host, user=name, passwd=password,  
db=db_name, connect_timeout=5)  
#Perform some Processing reading data from the RDS database  
#Code Block  
#Code Block  
#Code Block
```

What two actions can be taken to improve the performance of this Lambda function without increasing the cost of the solution? (Select two.)

- A. Package only the modules the Lambda function requires
- B. Use Amazon DynamoDB instead of Amazon RDS
- C. Move the initialization of the variable Amazon RDS connection outside of the handler function
- D. Implement custom database connection pooling with the Lambda function
- E. Implement local caching of Amazon RDS data so Lambda can re-use the cache

Answer: AC

Question #42

An application will ingest data at a very high throughput from many sources and must store the data in an Amazon S3 bucket. Which service would BEST accomplish this task?

- A. Amazon Kinesis Firehose
- B. Amazon S3 Acceleration Transfer

<https://itexamcertified.com>

- C. Amazon SQS
- D. Amazon SNS

Answer: A

Question #43

A Developer has setup an Amazon Kinesis Stream with 4 shards to ingest a maximum of 2500 records per second. A Lambda function has been configured to process these records.

In which order will these records be processed?

- A. Lambda will receive each record in the reverse order it was placed into the stream following a LIFO (last-in, first-out) method
- B. Lambda will receive each record in the exact order it was placed into the stream following a FIFO (first-in, first-out) method.
- C. Lambda will receive each record in the exact order it was placed into the shard following a FIFO (first-in, first-out) method. There is no guarantee of order across shards.
- D. The Developer can select FIFO, (first-in, first-out), LIFO (last-in, last-out), random, or request specific record using the getRecords API.

Answer: C

Question #44

A static website is hosted in an Amazon S3 bucket. Several HTML pages on the site use JavaScript to download images from another Amazon S3 bucket. These images are not displayed when users browse the site.

What is the possible cause for the issue?

- A. The referenced Amazon S3 bucket is in another region.
- B. The images must be stored in the same Amazon S3 bucket.
- C. Port 80 must be opened on the security group in which the Amazon S3 bucket is located.
- D. Cross Origin Resource Sharing must be enabled on the Amazon S3 bucket.

Answer: D

Question #45

Amazon S3 has the following structure: S3://BUCKET/FOLDERNAME/FILENAME.zip

<https://itexamcertified.com>

<https://itexamcertified.com>

Which S3 best practice would optimize performance with thousands of PUT request each second to a single bucket?

- A. Prefix folder names with user id; for example, s3://BUCKET/2013-FOLDERNAME/FILENAME.zip
- B. Prefix file names with timestamps; for example, s3://BUCKET/FOLDERNAME/2013-26-05-15-00-00-FILENAME.zip
- C. Prefix file names with random hex hashes; for example, s3://BUCKET/FOLDERNAME/23a6-FILENAME.zip
- D. Prefix folder names with random hex hashes; for example, s3://BUCKET/23a6-FOLDERNAME/FILENAME.zip

Answer: D

Reference:

<http://jayendrapatil.com/aws-s3-best-practices/>

Question #46

For a deployment using AWS CodeDeploy, what is the run order of the hooks for in-place deployments?

- A. Before Install -> Application Stop -> Application Start -> After Install
- B. Application Stop -> Before Install -> After Install -> Application Start
- C. Before Install -> Application Stop -> Validate Service -> Application Start
- D. Application Stop -> Before Install -> Validate Service -> Application Start

Answer: B

Reference:

<https://docs.aws.amazon.com/codedeploy/latest/userguide/reference-appspec-file-structure-hooks.html>

Question #47

A Developer is developing an application that manages financial transactions. To improve security, multi-factor authentication (MFA) will be required as part of the login protocol.

What services can the Developer use to meet these requirements?

- A. Amazon DynamoDB to store MFA session data, and Amazon SNS to send MFA codes
- B. Amazon Cognito with MFA
- C. AWS Directory Service
- D. AWS IAM with MFA enabled

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: D

Reference:

<https://aws.amazon.com/iam/details/mfa/>

Question #48

A game stores user game data in an Amazon DynamoDB table. Individual users should not have access to other users' game data. How can this be accomplished?

- A. Encrypt the game data with individual user keys.
- B. Restrict access to specific items based on certain primary key values.
- C. Stage data in SQS queues to inject metadata before accessing DynamoDB.
- D. Read records from DynamoDB and discard irrelevant data client-side.

Answer: B

Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/specifying-conditions.html>

Question #49

A company developed a set of APIs that are being served through the Amazon API Gateway. The API calls need to be authenticated based on OpenID identity providers such as Amazon or Facebook. The APIs should allow access based on a custom authorization model.

Which is the simplest and MOST secure design to use to build an authentication and authorization model for the APIs?

- A. Use Amazon Cognito user pools and a custom authorizer to authenticate and authorize users based on JSON Web Tokens.
- B. Build a OpenID token broker with Amazon and Facebook. Users will authenticate with these identify providers and pass the JSON Web Token to the API to authenticate each API call.
- C. Store user credentials in Amazon DynamoDB and have the application retrieve temporary credentials from AWS STS. Make API calls by passing user credentials to the APIs for authentication and authorization.
- D. Use Amazon RDS to store user credentials and pass them to the APIs for authentications and authorization.

Answer: A

Question #50

<https://itexamcertified.com>

<https://itexamcertified.com>

A supplier is writing a new RESTful API for customers to query the status of orders. The customers requested the following API endpoint. <http://www.supplierdomain.com/status/customerID>

Which of the following application designs meet the requirements? (Select two.)

- A. Amazon SQS; Amazon SNS
- B. Elastic Load Balancing; Amazon EC2
- C. Amazon ElastiCache; Amazon Elasticsearch Service
- D. Amazon API Gateway; AWS Lambda
- E. Amazon S3; Amazon CloudFront

Answer:BD

Question #51

A development team consists of 10 team members. Similar to a home directory for each team member the manager wants to grant access to user-specific folders in an Amazon S3 bucket. For the team member with the username "TeamMemberX", the snippet of the IAM policy looks like this:

```
{"Sid": "AllowS3ActionToFolders", "Effect": "Allow", "Action":  
["s3:*"], "Resource":  
["arn:aws:s3:::companyname/home/TeamMemberX/*"] }
```

Instead of creating distinct policies for each team member, what approach can be used to make this policy snippet generic for all team members?

- A. Use IAM policy condition
- B. Use IAM policy principal
- C. Use IAM policy variables
- D. Use IAM policy resource

Answer: C

Question #52

A legacy service has an XML-based SOAP interface. The Developer wants to expose the functionality of the service to external clients with the Amazon API

Gateway. Which technique will accomplish this?

- A. Create a RESTful API with the API Gateway; transform the incoming JSON into a valid XML message for the SOAP interface using mapping templates.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Create a RESTful API with the API Gateway; pass the incoming JSON to the SOAP interface through an Application Load Balancer.
- C. Create a RESTful API with the API Gateway; pass the incoming XML to the SOAP interface through an Application Load Balancer.
- D. Create a RESTful API with the API Gateway; transform the incoming XML into a valid message for the SOAP interface using mapping templates.

Answer: A

Question #53

A company is using AWS CodeBuild to compile a website from source code stored in AWS CodeCommit. A recent change to the source code has resulted in the

CodeBuild project being unable to successfully compile the website.

How should the Developer identify the cause of the failures?

- A. Modify the buildspec.yml file to include steps to send the output of build commands to Amazon CloudWatch.
- B. Use a custom Docker image that includes the AWS X-Ray agent in the AWS CodeBuild project configuration.
- C. Check the build logs of the failed phase in the last build attempt in the AWS CodeBuild project build history.
- D. Manually re-run the build process on a local machine so that the output can be visualized.

Answer: C

Question #54

A web application is using Amazon Kinesis Streams for clickstream data that may not be consumed for up to 12 hours.

How can the Developer implement encryption at rest for data within the Kinesis Streams?

- A. Enable SSL connections to Kinesis
- B. Use Amazon Kinesis Consumer Library
- C. Encrypt the data once it is at rest with a Lambda function
- D. Enable server-side encryption in Kinesis Streams

Answer: D

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

<https://aws.amazon.com/about-aws/whats-new/2017/07/amazon-kinesis-streams-introduces-server-side-encryption/>

Question #55

A Developer wants to use AWS X-Ray to trace a user request end-to-end throughput the software stack. The Developer made the necessary changes in the application tested it, and found that the application is able to send the traces to AWS X-Ray. However, when the application is deployed to an EC2 instance, the traces are not available.

Which of the following could create this situation? (Select two.)

- A. The traces are reaching X-Ray, but the Developer does not have access to view the records.
- B. The X-Ray daemon is not installed on the EC2 instance.
- C. The X-Ray endpoint specified in the application configuration is incorrect.
- D. The instance role does not have "xray:BatchGetTraces" and "xray:GetTraceGraph" permissions.
- E. The instance role does not have "xray:PutTraceSegments" and "xray:PutTelemetryRecords" permissions.

Answer: BE

Question #56

A Developer executed a AWS CLI command and received the error shown below:

```
A client error (UnauthorizedOperation) occurred when calling the RunInstances operation:  
You are not authorized to perform this operation. Encoded authorization failure message:  
oGsbAaIV7wlfj8zUqebHUANHzFbmkzILLxyj_y9xwhIHk99U_cUq1FIeZnskWDjQ1wSHStVfdCEyZILGoccGpCic  
IhORceWF9rRwFTnEcRJ3N9iTrPAE1WHveC5Z54ALPaW1EjH1Lg8CaB8d81CKmxQuylCm0r1Bf2fHJRUjAYopMVmg  
8olFmKA19yn_Z5rI120Q9p5ZIMX28zM4dTu1cJQUQjosgrEejfiIMYDda817Ooko9H6VmGJX62KfkRa517yE6hhh  
2bIwA6tpyCJy2LWFRTe4bafqAy0qkarhPA4mGiZyWn4gSqb08o-  
uqSIvWYPweaKGkampa0arcFR4gBD7Ph097WYBkzX9hVjGppLMy4jpXRv
```

What action should the Developer perform to make this error human-readable?

- A. Make a call to AWS KMS to decode the message.
- B. Use the AWS STS decode-authorization-message API to decode the message.
- C. Use an open source decoding library to decode the message.
- D. Use the AWS IAM decode-authorization-message API to decode this message.

Answer: B

<https://itexamcertified.com>

Question #57

A company is using Amazon API Gateway to manage access to a set of microservices implemented as AWS Lambda functions. Following a bug report, the company makes a minor breaking change to one of the APIs.

In order to avoid impacting existing clients when the new API is deployed, the company wants to allow clients six months to migrate from v1 to v2.

Which approach should the Developer use to handle this change?

- A. Update the underlying Lambda function and provide clients with the new Lambda invocation URL.
- B. Use API Gateway to automatically propagate the change to clients, specifying 180 days in the phased deployment parameter.
- C. Use API Gateway to deploy a new stage named v2 to the API and provide users with its URL.
- D. Update the underlying Lambda function, create an Amazon CloudFront distribution with the updated Lambda function as its origin.

Answer: C

Question #58

A company has written a Java AWS Lambda function to be triggered whenever a user uploads an image to an Amazon S3 bucket. The function converts the original image to several different formats and then copies the resulting images to another Amazon S3 bucket.

The Developers find that no images are being copied to the second Amazon S3 bucket. They have tested the code on an Amazon EC2 instance with 1GB of

RAM, and it takes an average of 500 seconds to complete.

What is the MOST likely cause of the problem?

- A. The Lambda function has insufficient memory and needs to be increased to 1 GB to match the Amazon EC2 instance
- B. Files need to be copied to the same Amazon S3 bucket for processing, so the second bucket needs to be deleted.
- C. Lambda functions have a maximum execution limit of 300 seconds, therefore the function is not completing.
- D. There is a problem with the Java runtime for Lambda, and the function needs to be converted to node.js. C

Answer: C

Question #59

An application stops working with the following error: The specified bucket does not exist. Where is the BEST place to start the root cause analysis?

<https://itexamcertified.com>

- A. Check the Elastic Load Balancer logs for DeleteBucket requests.
- B. Check the application logs in Amazon CloudWatch Logs for Amazon S3 DeleteBucket errors.
- C. Check AWS X-Ray for Amazon S3 DeleteBucket alarms.
- D. Check AWS CloudTrail for a DeleteBucket event.

Answer: D

Reference:

<https://github.com/serverless/serverless-graphql/issues/72>

Question #60

An organization must store thousands of sensitive audio and video files in an Amazon S3 bucket. Organizational security policies require that all data written to this bucket be encrypted.

How can compliance with this policy be ensured?

- A. Use AWS Lambda to send notifications to the security team if unencrypted objects are put in the bucket.
- B. Configure an Amazon S3 bucket policy to prevent the upload of objects that do not contain the x-amz-server-side-encryption header.
- C. Create an Amazon CloudWatch event rule to verify that all objects stored in the Amazon S3 bucket are encrypted.
- D. Configure an Amazon S3 bucket policy to prevent the upload of objects that contain the x-amz-server-side-encryption header.

Answer: B

Question #61

An application overwrites an object in Amazon S3, and then immediately reads the same object. Why would the application sometimes retrieve the old version of the object?

- A. S3 overwrite PUTS are eventually consistent, so the application may read the old object.
- B. The application needs to add extra metadata to label the latest version when uploading to Amazon S3.
- C. All S3 PUTS are eventually consistent, so the application may read the old object.
- D. The application needs to explicitly specify latest version when retrieving the object.

Answer: A

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #62

The release process workflow of an application requires a manual approval before the code is deployed into the production environment.

What is the BEST way to achieve this using AWS CodePipeline?

- A. Use multiple pipelines to allow approval
- B. Use an approval action in a stage
- C. Disable the stage transition to allow manual approval
- D. Disable a stage just prior the deployment stage

Answer: B

Question #63

Where should the appspec.yml file be placed in order for AWS CodeDeploy to work?

- A. In the root of the application source code directory structure
- B. In the bin folder along with all the complied code
- C. In an S3 bucket
- D. In the same folder as the application configuration files

Answer: A

Reference:

<https://docs.aws.amazon.com/codedeploy/latest/userguide/reference-appspec-file.html>

Question #64

An existing serverless application processes uploaded image files. The process currently uses a single Lambda function that takes an image file, performs the processing, and stores the file in Amazon S3. Users of the application now require thumbnail generation of the images. Users want to avoid any impact to the time it takes to perform the image uploads.

How can thumbnail generation be added to the application, meeting user requirements while minimizing changes to existing code?

- A. Change the existing Lambda function handling the uploads to create thumbnails at the time of upload. Have the function store both the image and thumbnail in Amazon S3.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Create a second Lambda function that handles thumbnail generation and storage. Change the existing Lambda function to invoke it asynchronously.
- C. Create an S3 event notification with a Lambda function destination. Create a new Lambda function to generate and store thumbnails.
- D. Create an S3 event notification to an SQS Queue. Create a scheduled Lambda function that processes the queue, and generates and stores thumbnails.

Answer: C

Reference:

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

Question #65

A Developer must re-implement the business logic for an order fulfilment system. The business logic has to make requests to multiple vendors to decide where to purchase an item. The whole process can take up to a week to complete.

What is the MOST efficient and SIMPLEST way to implement a system that meets these requirements?

- A. Use AWS Step Functions to execute parallel Lambda functions, and join the results.
- B. Create an AWS SQS for each vendor, poll the queue from a worker instance, and joint the results.
- C. Use AWS Lambda to asynchronously call a Lambda function for each vendor, and join the results.
- D. Use Amazon CloudWatch Events to orchestrate the Lambda functions.

Answer: A

Question #66

A customer wants to deploy its source code on an AWS Elastic Beanstalk environment. The customer needs to perform deployment with minimal outage and should only use existing instances to retain application access log.

What deployment policy would satisfy these requirements?

- A. Rolling
- B. All at once
- C. Rolling with an additional batch
- D. Immutable

Answer: A

<https://itexamcertified.com>

<https://itexamcertified.com>

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rollingupdates.html>

Question #67

A Developer has been asked to build a real-time dashboard web application to visualize the key prefixes and storage size of objects in Amazon S3 buckets.

Amazon DynamoDB will be used to store the Amazon S3 metadata.

What is the optimal and MOST cost-effective design to ensure that the real-time dashboard is kept up to date with the state of the objects in the Amazon S3 buckets?

- A. Use an Amazon CloudWatch event backed by an AWS Lambda function. Issue an Amazon S3 API call to get a list of all Amazon S3 objects and persist the metadata within DynamoDB. Have the web application poll the DynamoDB table to reflect this change.
- B. Use Amazon S3 Event Notification backed by a Lambda function to persist the metadata into DynamoDB. Have the web application poll the DynamoDB table to reflect this change.
- C. Run a cron job within an Amazon EC2 instance to list all objects within Amazon S3 and persist the metadata into DynamoDB. Have the web application poll the DynamoDB table to reflect this change.
- D. Create a new Amazon EMR cluster to get all the metadata about Amazon S3 objects; persist the metadata into DynamoDB. Have the web application poll the DynamoDB table to reflect this change. A

Correct Answe : B

Question #68

A Developer must repeatedly and consistently deploy a serverless RESTful API on AWS.

Which techniques will work? (Choose two.)

- A. Define a Swagger file. Use AWS Elastic Beanstalk to deploy the Swagger file.
- B. Define a Swagger file. Use AWS CodeDeploy to deploy the Swagger file.
- C. Deploy a SAM template with an inline Swagger definition.
- D. Define a Swagger file. Deploy a SAM template that references the Swagger file.
- E. Define an inline Swagger definition in a Lambda function. Invoke the Lambda function.

Answer: DE

Question #69

<https://itexamcertified.com>

A set of APIs are exposed to customers using the Amazon API Gateway. These APIs have caching enabled on the API Gateway. Customers have asked for an option to invalidate this cache for each of the APIs.

What action can be taken to allow API customers to invalidate the API Cache?

- A. Ask customers to use AWS credentials to call the InvalidateCache API.
- B. Ask customers to invoke an AWS API endpoint which invalidates the cache.
- C. Ask customers to pass an HTTP header called Cache-Control:max-age=0.
- D. Ask customers to add a query string parameter called "INVALIDATE_CACHE" when making an API call.

Answer: C

Question #70

A Developer uses AWS CodeDeploy to automate application deployment that connects to an external MySQL database. The Developer wants to securely access the encrypted secrets, such as API keys and database passwords.

Which of the following solutions would involve the LEAST administrative effort?

- A. Save the secrets in Amazon S3 with AWS KMS server-side encryption, and use a signed URL to access them by using the IAM role from Amazon EC2 instances.
- B. Use the instance metadata to store the secrets and to programmatically access the secrets from EC2 instances.
- C. Use the Amazon DynamoDB client-side encryption library to save the secrets in DynamoDB and to programmatically access the secrets from EC2 instances.
- D. Use AWS SSM Parameter Store to store the secrets and to programmatically access them by using the IAM role from EC2 instances.

Answer: D

Question #71

An application running on EC2 instances is storing data in an S3 bucket. Security policy mandates that all data must be encrypted in transit.

How can the Developer ensure that all traffic to the S3 bucket is encrypted?

- A. Install certificates on the EC2 instances.
- B. Create a bucket policy that allows traffic where SecureTransport is true.
- C. Create an HTTPS redirect on the EC2 instances.
- D. Create a bucket policy that denies traffic where SecureTransport is false.

<https://itexamcertified.com>

Answer: D

Question #72

A company is developing a new online game that will run on top of Amazon ECS. Four distinct Amazon ECS services will be part of the architecture, each requiring specific permissions to various AWS services. The company wants to optimize the use of the underlying Amazon EC2 instances by bin packing the containers based on memory reservation.

Which configuration would allow the Development team to meet these requirements MOST securely?

- A. Create a new Identity and Access Management (IAM) instance profile containing the required permissions for the various ECS services, then associate that instance role with the underlying EC2 instances.
- B. Create four distinct IAM roles, each containing the required permissions for the associated ECS service, then configure each ECS service to reference the associated IAM role.
- C. Create four distinct IAM roles, each containing the required permissions for the associated ECS service, then, create an IAM group and configure the ECS cluster to reference that group.
- D. Create four distinct IAM roles, each containing the required permissions for the associated ECS service, then configure each ECS task definition to reference the associated IAM role.

Answer: D

Question #73

A company needs to encrypt data at rest, but it wants to leverage an AWS managed service using its own master key.

Which of the following AWS service can be used to meet these requirements?

- A. SSE with Amazon S3
- B. SSE with AWS KMS
- C. Client-side encryption
- D. AWS IAM roles and policies

Answer: B

Question #74

When a Developer tries to run an AWS CodeBuild project, it raises an error because the length of all environment variables exceeds the limit for the combined maximum of characters.

<https://itexamcertified.com>

<https://itexamcertified.com>

What is the recommended solution?

- A. Add the export LC_ALL="en_US.utf8" command to the pre_build section to ensure POSIX localization.
- B. Use Amazon Cognito to store key-value pairs for large numbers of environment variables.
- C. Update the settings for the build project to use an Amazon S3 bucket for large numbers of environment variables.
- D. Use AWS Systems Manager Parameter Store to store large numbers of environment variables.

Answer: D

Reference:

<https://docs.aws.amazon.com/codebuild/latest/userguide/troubleshooting.html>

Question #75

A Lambda function is packaged for deployment to multiple environments, including development, test, production, etc. Each environment has unique set of resources such as databases, etc.

How can the Lambda function use the resources for the current environment?

- A. Apply tags to the Lambda functions.
- B. Hardcore resources in the source code.
- C. Use environment variables for the Lambda functions.
- D. Use separate function for development and production.

Answer: C

Question #76

The Developer for a retail company must integrate a fraud detection solution into the order processing solution. The fraud detection solution takes between ten and thirty minutes to verify an order. At peak, the web site can receive one hundred orders per minute.

What is the most scalable method to add the fraud detection solution to the order processing pipeline?

- A. Add all new orders to an Amazon SQS queue. Configure a fleet of 10 EC2 instances spanning multiple AZs with the fraud detection solution installed on them to pull orders from this queue. Update the order with a pass or fails status.
- B. Add all new orders to an SQS queue. Configure an Auto Scaling group that uses the queue depth metric as its unit of scale to launch a dynamically-sized fleet of EC2 instances spanning multiple AZs with the fraud detection solution installed on them to pull orders from this queue. Update the order with a pass or fails status.

<https://itexamcertified.com>

<https://itexamcertified.com>

C. Add all new orders to an Amazon Kinesis Stream. Subscribe a Lambda function to automatically read batches of records from the Kinesis Stream. The Lambda function includes the fraud detection software and will update the order with a pass or fail status.

D. Write all new orders to Amazon DynamoDB. Configure DynamoDB Streams to include all new orders. Subscribe a Lambda function to automatically read batches of records from the Kinesis Stream. The Lambda function includes the fraud detection software and will update the order with a pass or fail status.

Answer: B

Question #77

A Developer is creating a mobile application with a limited budget. The solution requires a scalable service that will enable customers to sign up and authenticate into the mobile application while using the organization's current SAML 2.0 identity provider.

Which AWS service should be used to meet these requirements?

- A. AWS Lambda
- B. Amazon Cognito
- C. AWS IAM
- D. Amazon EC2

Answer: B

Question #78

An application is real-time processing millions of events that are received through an API.

What service could be used to allow multiple consumers to process the data concurrently and MOST cost-effectively?

- A. Amazon SNS with fanout to an SQS queue for each application
- B. Amazon SNS with fanout to an SQS FIFO (first-in, first-out) queue for each application
- C. Amazon Kinesis Firehouse
- D. Amazon Kinesis Streams

Answer: D

Reference:

<https://aws.amazon.com/kinesis/data-streams/getting-started/>

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #79

A Developer needs to use AWS X-Ray to monitor an application that is deployed on EC2 instances.

What steps have to be executed to perform the monitoring?

- A. Deploy the X-Ray SDK with the application and use X-Ray annotation.
- B. Install the X-Ray daemon and instrument the application code.
- C. Install the X-Ray daemon and configure it to forward data to Amazon CloudWatch Events.
- D. Deploy the X-Ray SDK with the application and instrument the application code.

Answer: B

Reference:

<https://aws.amazon.com/blogs/aws/category/aws-x-ray/>

Question #80

A Developer will be using the AWS CLI on a local development server to manage AWS services.

What can be done to ensure that the CLI uses the Developer's IAM permissions when making commands?

- A. Specify the Developer's IAM access key ID and secret access key as parameters for each CLI command.
- B. Run the aws configure CLI command, and provide the Developer's IAM access key ID and secret access key.
- C. Specify the Developer's IAM user name and password as parameters for each CLI command.
- D. Use the Developer's IAM role when making the CLI command. B

Answer: B

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/iam-assume-role-cli/>

Question #81

After installing the AWS CLI, a Developer tries to run the command aws configure but receives the following error:

Error: aws: command not found -

What is the most likely cause of this error?

- A. The aws executable is not in the PATH environment variable.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Access to the aws executable has been denied to the installer.
- C. Incorrect AWS credentials were provided.
- D. The aws script does not have an executable file mode.

Answer: A

Reference:

<https://docs.aws.amazon.com/cli/latest/userguide/troubleshooting.html>

Question #82

An on-premises legacy application is caching data files locally and writing shared images to local disks.

What is necessary to allow for horizontal scaling when migrating the application to AWS?

- A. Modify the application to have both shared images and caching data written to Amazon EBS.
- B. Modify the application to read and write cache data on Amazon S3, and also store shared images on S3.
- C. Modify the application to use Amazon S3 for serving shared images; cache data can then be written to local disks.
- D. Modify the application to read and write cache data on Amazon S3, while continuing to write shared images to local disks.

Answer: C

Question #83

A Developer must trigger an AWS Lambda function based on the item lifecycle activity in an Amazon DynamoDB table.

How can the Developer create the solution?

- A. Enable a DynamoDB stream that publishes an Amazon SNS message. Trigger the Lambda function synchronously from the SNS message.
- B. Enable a DynamoDB stream that publishes an SNS message. Trigger the Lambda function asynchronously from the SNS message.
- C. Enable a DynamoDB stream, and trigger the Lambda function synchronously from the stream.
- D. Enable a DynamoDB stream, and trigger the Lambda function asynchronously from the stream.

Answer: C

<https://itexamcertified.com>

<https://itexamcertified.com>

Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html>

Question #84

A gaming company is developing a mobile game application for iOS® and Android® platforms. This mobile game securely stores user data locally on the device.

The company wants to allow users to use multiple device for the game, which requires user data synchronization across device.

Which service should be used to synchronize user data across devices without the need to create a backend application?

- A. AWS Lambda
- B. Amazon S3
- C. Amazon DynamoDB
- D. Amazon Cognito

Answer: D

Reference:

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-sync.html>

Question #85

An on-premises application is implemented using a Linux, Apache, MySQL and PHP (LAMP) stack. The Developer wants to run this application in AWS.

Which of the following sets of AWS services can be used to run this stack?

- A. Amazon API Gateway, Amazon S3
- B. AWS Lambda, Amazon DynamoDB
- C. Amazon EC2, Amazon Aurora
- D. Amazon Cognito, Amazon RDS
- E. Amazon ECS, Amazon EBS

Answer: C

Reference:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/php-ha-tutorial.html?icmpid=docs_tutorial_projects

<https://itexamcertified.com>

Question #86

An application displays a status dashboard. The status is updated by 1 KB messages from an SQS queue. Although the status changes infrequently, the

Developer must minimize the time between the message arrival in the queue and the dashboard update.

What technique provides the shortest delay in updating the dashboard?

- A. Retrieve the messages from the queue using long polling every 20 seconds.
- B. Reduce the size of the messages by compressing them before sending.
- C. Retrieve the messages from the queue using short polling every 10 seconds.
- D. Reduce the size of each message payload by sending it in two parts. A

Answer: A

Question #87

A company is using AWS CodePipeline to deliver one of its applications. The delivery pipeline is triggered by changes to the master branch of an AWS

CodeCommit repository and uses AWS CodeBuild to implement the test and build stages of the process and AWS CodeDeploy to deploy the application.

The pipeline has been operating successfully for several months and there have been no modifications. Following a recent change to the application's source code, AWS CodeDeploy has not deployed the updates application as expected.

What are the possible causes? (Choose two.)

- A. The change was not made in the master branch of the AWS CodeCommit repository.
- B. One of the earlier stages in the pipeline failed and the pipeline has terminated.
- C. One of the Amazon EC2 instances in the company's AWS CodePipeline cluster is inactive.
- D. The AWS CodePipeline is incorrectly configured and is not executing AWS CodeDeploy.
- E. AWS CodePipeline does not have permissions to access AWS CodeCommit.

Answer: AB

Question #88

A social media company is using Amazon Cognito in order to synchronize profiles across different mobile devices, to enable end users to have a seamless experience.

<https://itexamcertified.com>

Which of the following configurations can be used to silently notify users whenever an update is available on all other devices?

- A. Modify the user pool to include all the devices which keep them in sync.
- B. Use the SyncCallback interface to receive notifications on the application.
- C. Use an Amazon Cognito stream to analyze the data and push the notifications.
- D. Use the push synchronization feature with the appropriate IAM role.

Answer: D

Reference:

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-sync.html>

Question #89

A website's page load times are gradually increasing as more users access the system at the same time. Analysis indicates that a user profile is being loaded from a database in all the web pages being visited by each user and this is increasing the database load and the page load latency. To address this issue the

Developer decides to cache the user profile data.

Which caching strategy will address this situation MOST efficiently?

- A. Create a new Amazon EC2 Instance and run a NoSQL database on it. Cache the profile data within this database using the write-through caching strategy.
- B. Create an Amazon ElastiCache cluster to cache the user profile data. Use a cache-aside caching strategy.
- C. Use a dedicated Amazon RDS instance for caching profile data. Use a write-through caching strategy.
- D. Create an ElastiCache cluster to cache the user profile data. Use a write-through caching strategy.

Answer: B

Question #90

An application needs to use the IP address of the client in its processing. The application has been moved into AWS and has been placed behind an Application Load Balancer (ALB). However, all the client IP addresses now appear to be the same. The application must maintain the ability to scale horizontally.

Based on this scenario, what is the MOST cost-effective solution to this problem?

- A. Remove the application from the ALB. Delete the ALB and change Amazon Route 53 to direct traffic to the instance running the application.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Remove the application from the ALB. Create a Classic Load Balancer in its place. Direct traffic to the application using the HTTP protocol.
- C. Alter the application code to inspect the X-Forwarded-For header. Ensure that the code can work properly if a list of IP addresses is passed in the header.
- D. Alter the application code to inspect a custom header. Alter the client code to pass the IP address in the custom header.

Answer: C

Question #91

A development team is using AWS Elastic Beanstalk to deploy a two-tier application that consists of a load-balanced web tier and an Amazon RDS database tier in production. The team would like to separate the RDS instance from the Elastic Beanstalk.

How can this be accomplished?

- A. Use the Elastic Beanstalk CLI to disassociate the database.
- B. Use the AWS CLI to disassociate the database.
- C. Change the deployment policy to disassociate the database.
- D. Recreate a new Elastic Beanstalk environment without Amazon RDS. C

Answer: D

Question #92

According to best practice, how should access keys be managed in AWS? (Choose two.)

- A. Use the same access key in all applications for consistency.
- B. Delete all access keys for the account root user.
- C. Leave unused access keys in the account for tracking purposes.
- D. Embed and encrypt access keys in code for continuous deployment.
- E. Use Amazon IAM roles instead of access keys where possible.

Answer: BE

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

<https://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html#iam-user-access-keys>

Question #93

The development team is working on an API that will be served from Amazon API gateway. The API will be served from three environments: development, test, and production. The API Gateway is configured to use 237 GB of cache in all three stages.

Which is the MOST cost-efficient deployment strategy?

- A. Create a single API Gateway with all three stages.
- B. Create three API Gateways, one for each stage in a single AWS account.
- C. Create an API Gateway in three separate AWS accounts.
- D. Enable the cache for development and test environments only when needed.

Answer: A

Question #94

An application running on an Amazon Linux EC2 instance needs to manage the AWS infrastructure.

How can the EC2 instance be configured to make AWS API calls securely?

- A. Sign the AWS CLI command using the signature version 4 process.
- B. Run the aws configure AWS CLI command and specify the access key id and secret access key.
- C. Specify a role for the EC2 instance with the necessary privileges.
- D. Pass the access key id and secret access key as parameters for each AWS CLI command.

Answer: C

Question #95

A company is migrating from a monolithic architecture to a microservices-based architecture. The Developers need to refactor the application so that the many microservices can asynchronously communicate with each other without impacting performance.

Use of which managed AWS services will enable asynchronous message passing? (Choose two.)

- A. Amazon SQS
- B. Amazon Cognito
- C. Amazon Kinesis

<https://itexamcertified.com>

<https://itexamcertified.com>

- D. Amazon SNS
- E. Amazon ElastiCache

Answer: AD

Question #96

An application runs on multiple EC2 instances behind an ELB.

Where is the session data best written so that it can be served reliably across multiple requests?

- A. Write data to Amazon ElastiCache
- B. Write data to Amazon Elastic Block Store.
- C. Write data to Amazon EC2 Instance Store.
- D. Write data to the root filesystem.

Answer: A

Reference:

https://docs.aws.amazon.com/awstechnicalcontent/latest/microservices-on-aws/microservices-on-aws.pdf?icmpid=link_from_whitepapers_page

(14)

Question #97

A Developer is creating a Lambda function that will generate and export a file. The function requires 100 MB of temporary storage for temporary files while executing. These files will not be needed after the function is complete.

How can the Developer MOST efficiently handle the temporary files?

- A. Store the files in EBS and delete the files at the end of the Lambda function.
- B. Copy the files to EFS and delete the files at the end of the Lambda function.
- C. Store the files in the /tmp directory and delete the files at the end of the Lambda function.
- D. Copy the files to an S3 bucket with a lifecycle policy to delete the files.

Answer: C

Reference:

<https://forums.aws.amazon.com/thread.jspa?threadID=174119>

<https://itexamcertified.com>

Question #98

A Developer has developed a web application and wants to deploy it quickly on a Tomcat server on AWS. The Developer wants to avoid having to manage the underlying infrastructure.

What is the easiest way to deploy the application, based on these requirements?

- A. AWS CloudFormation
- B. AWS Elastic Beanstalk
- C. Amazon S3
- D. AWS CodePipeline

Answer: B

Reference:

<https://aws.amazon.com/answers/web-applications/aws-web-app-deployment-javascript/>

Question #99

An application uses Lambda functions to extract metadata from files uploaded to an S3 bucket; the metadata is stored in Amazon DynamoDB. The application starts behaving unexpectedly, and the Developer wants to examine the logs of the Lambda function code for errors.

Based on this system configuration, where would the Developer find the logs?

- A. Amazon S3
- B. AWS CloudTrail
- C. Amazon CloudWatch
- D. Amazon DynamoDB

Answer: C

Question #100

An organization is using Amazon CloudFront to ensure that its users experience low-latency access to its web application. The organization has identified a need to encrypt all traffic between users and CloudFront, and all traffic between CloudFront and the web application.

How can these requirements be met? (Choose two.)

- A. Use AWS KMS to encrypt traffic between CloudFront and the web application.

<https://itexamcertified.com>

- B. Set the Origin Protocol Policy to "HTTPS Only".
- C. Set the Origin's HTTP Port to 443.
- D. Set the Viewer Protocol Policy to "HTTPS Only" or "Redirect HTTP to HTTPS".
- E. Enable the CloudFront option Restrict Viewer Access.

Answer: BD

Question #101

An application is using Amazon DynamoDB as its data store, and should be able to read 100 items per second as strongly consistent reads. Each item is 5 KB in size.

To what value should the table's provisioned read throughput be set?

- A. 50 read capacity units
- B. 100 read capacity units
- C. 200 read capacity units
- D. 500 read capacity units

Answer: C

Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

Question #102

A web application is designed to allow new users to create accounts using their email addresses. The application will store attributes for each user, and is expecting millions of user to sign up.

What should the Developer implement to achieve the design goals?

- A. Amazon Cognito user pools
- B. AWS Mobile Hub user data storage
- C. Amazon Cognito Sync
- D. AWS Mobile Hub cloud logic

Answer: A

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

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

Question #103

A company needs a new REST API that can return information about the contents of an Amazon S3 bucket, such as a count of the objects stored in it. The company has decided that the new API should be written as a microservice using AWS Lambda and Amazon API Gateway.

How should the Developer ensure that the microservice has the necessary access to the Amazon S3 bucket, while adhering to security best practices?

- A. Create an IAM user that has permissions to access the Amazon S3 bucket, and store the IAM user credentials in the Lambda function source code.
- B. Create an IAM role that has permissions to access the Amazon S3 bucket and assign it to the Lambda function as its execution role.
- C. Create an Amazon S3 bucket policy that specifies the Lambda service as its principal and assign it to the Amazon S3 bucket.
- D. Create an IAM role, attach the AmazonS3FullAccess managed policy to it, and assign the role to the Lambda function as its execution role.

Answer: C

Question #104

An application is running on an EC2 instance. The Developer wants to store an application metric in Amazon CloudWatch.

What is the best practice for implementing this requirement?

- A. Use the PUT Object API call to send data to an S3 bucket. Use an event notification to invoke a Lambda function to publish data to CloudWatch.
- B. Publish the metric data to an Amazon Kinesis Stream using a PutRecord API call. Subscribe a Lambda function that publishes data to CloudWatch.
- C. Use the CloudWatch PutMetricData API call to submit a custom metric to CloudWatch. Provide the required credentials to enable the API call.
- D. Use the CloudWatch PutMetricData API call to submit a custom metric to CloudWatch. Launch the EC2 instance with the required IAM role to enable the API call.

Answer: D

Reference:

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

<https://itexamcertified.com>

Question #105

Queries to an Amazon DynamoDB table are consuming a large amount of read capacity. The table has a significant number of large attributes. The application does not need all of the attribute data.

How can DynamoDB costs be minimized while maximizing application performance?

- A. Batch all the writes, and perform the write operations when no or few reads are being performed.
- B. Create a global secondary index with a minimum set of projected attributes.
- C. Implement exponential backoffs in the application.
- D. Load balance the reads to the table using an Application Load Balancer.

Answer: B

Question #106

AWS CodeBuild builds code for an application, creates the Docker image, pushes the image to Amazon Elastic Container Registry (Amazon ECR), and tags the image with a unique identifier.

If the Developers already have AWS CLI configured on their workstations, how can the Docker images be pulled to the workstations?

- A. Run the following: docker pull REPOSITORY URI : TAG
- B. Run the output of the following: aws ecr get-login and then run: docker pull REPOSITORY URI : TAG
- C. Run the following: aws ecr get-login and then run: docker pull REPOSITORY URI : TAG
- D. Run the output of the following: aws ecr get-download-url-for-layer and then run: docker pull REPOSITORY URI : TAG

Answer: B

Question #107

A company caches session information for a web application in an Amazon DynamoDB table. The company wants an automated way to delete old items from the table.

What is the simplest way to do this?

- A. Write a script that deletes old records; schedule the scripts as a cron job on an Amazon EC2 instance.
- B. Add an attribute with the expiration time; enable the Time To Live feature based on that attribute.
- C. Each day, create a new table to hold session data; delete the previous day's table.

<https://itexamcertified.com>

D. Add an attribute with the expiration time; name the attribute ItemExpiration.

Answer: B

Reference:

<https://aws.amazon.com/about-aws/whats-new/2017/02/amazon-dynamodb-now-supports-automatic-item-expiration-with-time-to-live-ttl/>

Question #108

An application is expected to process many files. Each file takes four minutes to process each AWS Lambda invocation. The Lambda function does not return any important data.

What is the fastest way to process all the files?

- A. First split the files to make them smaller, then process with synchronous RequestResponse Lambda invocations.
- B. Make synchronous RequestResponse Lambda invocations and process the files one by one.
- C. Make asynchronous Event Lambda invocations and process the files in parallel.
- D. First join all the files, then process it all at once with an asynchronous Event Lambda invocation.

Answer: C

Question #109

The upload of a 15 GB object to Amazon S3 fails. The error message reads: "Your proposed upload exceeds the maximum allowed object size."

What technique will allow the Developer to upload this object?

- A. Upload the object using the multi-part upload API.
- B. Upload the object over an AWS Direct Connect connection.
- C. Contact AWS Support to increase the object size limit.
- D. Upload the object to another AWS region.

Answer: A

Reference:

<https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-KACOEWK92oCmeCwuj4t/s3-question-on-multi-part-upload>

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #110

A company has an AWS CloudFormation template that is stored as a single file. The template is able to launch and create a full infrastructure stack.

Which best practice would increase the maintainability of the template?

- A. Use nested stacks for common template patterns.
- B. Embed credentials to prevent typos.
- C. Remove mappings to decrease the number of variables.
- D. Use AWS::Include to reference publicly-hosted template files.

Answer: A

Reference:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html>

Question #111

A Developer wants to encrypt new objects that are being uploaded to an Amazon S3 bucket by an application. There must be an audit trail of who has used the key during this process. There should be no change to the performance of the application.

Which type of encryption meets these requirements?

- A. Server-side encryption using S3-managed keys
- B. Server-side encryption with AWS KMS-managed keys
- C. Client-side encryption with a client-side symmetric master key
- D. Client-side encryption with AWS KMS-managed keys

Answer: B

Reference:

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

Question #112

An on-premises application makes repeated calls to store files to Amazon S3. As usage of the application has increased, "LimitExceeded" errors are being logged.

What should be changed to fix this error?

- A. Implement exponential backoffs in the application.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Load balance the application to multiple servers.
- C. Move the application to Amazon EC2.
- D. Add a one second delay to each API call.

Answer: A

Question #113

An organization is storing large files in Amazon S3, and is writing a web application to display meta-data about the files to end-users. Based on the metadata a user selects an object to download. The organization needs a mechanism to index the files and provide single-digit millisecond latency retrieval for the metadata.

What AWS service should be used to accomplish this?

- A. Amazon DynamoDB
- B. Amazon EC2
- C. AWS Lambda
- D. Amazon RDS

Answer: A

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed database and supports both document and key-value data models. Its flexible data model and reliable performance make it a great fit for mobile, web, gaming, ad-tech, Internet of Things (IoT), and many other applications.

Reference:

<https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/database-services.html>

Question #114

While developing an application that runs on Amazon EC2 in an Amazon VPC, a Developer identifies the need for centralized storage of application-level logs.

Which AWS service can be used to securely store these logs?

- A. Amazon EC2 VPC Flow Logs
- B. Amazon CloudWatch Logs
- C. Amazon CloudSearch
- D. AWS CloudTrail

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: B

Reference:

<https://aws.amazon.com/answers/logging/centralized-logging/>

Question #115

A stock market monitoring application uses Amazon Kinesis for data ingestion. During simulated tests of peak data rates, the Kinesis stream cannot keep up with the incoming data.

What step will allow Kinesis to accommodate the traffic during peak hours?

- A. Install the Kinesis Producer Library (KPL) for ingesting data into the stream.
- B. Reduce the data retention period to allow for more data ingestion using DecreaseStreamRetentionPeriod.
- C. Increase the shard count of the stream using UpdateShardCount.
- D. Ingest multiple records into the stream in a single call using PutRecords.

Answer: C

Reference:

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

Question #116

Where can PortMapping be defined when launching containers in Amazon ECS?

- A. Security groups
- B. Amazon Elastic Container Registry (Amazon ECR)
- C. Container agent
- D. Task definition

Answer: D

Reference:

https://docs.aws.amazon.com/AmazonECS/latest/userguide/task_definition_parameters.html

Question #117

An application uses Amazon Kinesis Data Streams to ingest and process large streams of data records in real time. Amazon EC2 instances consume and process the data from the shards of the Kinesis data stream by using Amazon Kinesis Client Library (KCL). The application handles the failure scenarios and does not require standby workers.

<https://itexamcertified.com>

<https://itexamcertified.com>

The application reports that a specific shard is receiving more data than expected. To adapt to the changes in the rate of data flow, the "hot" shard is resharded.

Assuming that the initial number of shards in the Kinesis data stream is 4, and after resharding the number of shards increased to 6, what is the maximum number of EC2 instances that can be deployed to process data from all the shards?

- A. 12
- B. 6
- C. 4
- D. 1

Answer: B

Question #118

A Development team is working on a case management solution that allows medical claims to be processed and reviewed. Users log in to provide information related to their medical and financial situations.

As part of the application, sensitive documents such as medical records, medical imaging, bank statements, and receipts are uploaded to Amazon S3. All documents must be securely transmitted and stored. All access to the documents must be recorded for auditing.

What is the MOST secure approach?

- A. Use S3 default encryption using Advanced Encryption Standard-256 (AES-256) on the destination bucket.
- B. Use Amazon Cognito for authorization and authentication to ensure the security of the application and documents.
- C. Use AWS Lambda to encrypt and decrypt objects as they are placed into the S3 bucket.
- D. Use client-side encryption/decryption with Amazon S3 and AWS KMS.

Answer: D

Question #119

A company has an internet-facing application that uses Web Identity Federation to obtain a temporary credential from AWS Security Token Service (AWS STS).

The app then uses the token to access AWS services.

Review the following response:

<https://itexamcertified.com>

<https://itexamcertified.com>

```
<AssumeRoleWithWebIdentityResponse xmlns="https://sts.amazonaws.com/doc/2011-06-15/">
  <AssumeRoleWithWebIdentityResult>
    <SubjectFromWebIdentityToken>amzn1.account.AF6RH07KZU5XRVQJGKK6HB56KR2A</SubjectFromWebIdentit
yToken>
    <Audience>client.5498841531868486423.1548@apps.example.com</Audience>
    <AssumedRoleUser>
      <Arn>arn:aws:sts::123456789012:assumed-role/FederatedWebIdentityRole/app1</Arn>
      <AssumedRoleId>AROACLWSDQRAOEXAMPLE:app1</AssumedRoleId>
    </AssumedRoleUser>
    <Credentials>
      <SessionToken>AQoDYKdzEE0a8ANXXXXXXXXXXXXNolewxE5TijQyp+IEXAMPLE</SessionToken>
      <SecretAccessKey>wJalrXutnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY</SecretAccessKey>
      <Expiration>2014-10-24T23:00:23Z</Expiration>
      <AccessKeyId>ASgeIAIOSFODNN7EXAMPLE</AccessKeyId>
    </Credentials>
    <Provider>www.amazon.com</Provider>
  </AssumeRoleWithWebIdentityResult>
  <ResponseMetadata>
    <RequestId>ad4156e9-bce1-11e2-82e6-6b6efEXAMPLE</RequestId>
  </ResponseMetadata>
</AssumeRoleWithWebIdentityResponse>
```

Based on the response displayed what permissions are associated with the call from the application?

- A. Permissions associated with the role AROACLWSDQRAOEXAMPLE:app1
- B. Permissions associated with the default role used when the AWS service was built
- C. Permission associated with the IAM principal that owns the AccessKeyID ASgeIAIOSFODNN7EXAMPLE
- D. Permissions associated with the account that owns the AWS service

Answer: A

Question #120

A Developer is using AWS CLI, but when running list commands on a large number of resources, it is timing out.

What can be done to avoid this time-out?

- A. Use pagination
- B. Use shorthand syntax
- C. Use parameter values
- D. Use quoting strings

Answer: A

Reference:

<https://docs.aws.amazon.com/cli/latest/userguide/cli-usage-pagination.html>

<https://itexamcertified.com>

Question #121

What does an Amazon SQS delay queue accomplish?

- A. Messages are hidden for a configurable amount of time when they are first added to the queue.
- B. Messages are hidden for a configurable amount of time after they are consumed from the queue.
- C. The consumer can poll the queue for a configurable amount of time before retrieving a message.
- D. Message cannot be deleted for a configurable amount of time after they are consumed from the queue.

Answer: A

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-delay-queues.html>

Question #122

A company has multiple Developers located across the globe who are updating code incrementally for a development project. When Developers upload code concurrently, internet connectivity is slow and it is taking a long time to upload code for deployment in AWS Elastic Beanstalk.

- Which step will result in minimized upload and deployment time with the LEAST amount of administrative effort?
- A. Allow the Developers to upload the code to an Amazon S3 bucket, and deploy it directly to Elastic Beanstalk.
 - B. Allow the Developers to upload the code to a central FTP server to deploy the application to Elastic Beanstalk.
 - C. Create an AWS CodeCommit repository, allow the Developers to commit code to it, and then directly deploy the code to Elastic Beanstalk.
 - D. Create a code repository on an Amazon EC2 instance so that all Developers can update the code, and deploy the application from the instance to Elastic Beanstalk.

Answer: C

Question #123

A company recently migrated its web, application and NoSQL database tiers to AWS. The company is using Auto Scaling to scale the web and application tiers.

More than 95 percent of the Amazon DynamoDB requests are repeated read-requests.

How can the DynamoDB NoSQL tier be scaled up to cache these repeated requests?

- A. Amazon EMR

<https://itexamcertified.com>

- B. Amazon DynamoDB Accelerator
- C. Amazon SQS
- D. Amazon CloudFront

Answer: B

Reference:

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

Question #124

A company is building an application to track athlete performance using an Amazon DynamoDB table. Each item in the table is identified by a partition key

(user_id) and a sort key (sport_name). The table design is shown below:

Partition Key: user_id
Sort Key: sport_name
Attributes: score
score_datetime

A Developer is asked to write a leaderboard application to display the top performers (user_id) based on the score for each sport_name.

What process will allow the Developer to extract results MOST efficiently from the DynamoDB table?

- A. Use a DynamoDB query operation with the key attributes of user_id and sport_name and order the results based on the score attribute.
- B. Create a global secondary index with a partition key of sport_name and a sort key of score, and get the results
- C. Use a DynamoDB scan operation to retrieve scores and user_id based on sport_name, and order the results based on the score attribute.
- D. Create a local secondary index with a primary key of sport_name and a sort key of score and get the results based on the score attribute.

Answer: B

Question #125

A Developer is creating a mobile application that will not require users to log in.

What is the MOST efficient method to grant users access to AWS resources?

- A. Use an identity provider to securely authenticate with the application.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Create an AWS Lambda function to create an IAM user when a user accesses the application.
- C. Create credentials using AWS KMS and apply these credentials to users when using the application.
- D. Use Amazon Cognito to associate unauthenticated users with an IAM role that has limited access to resources.

Answer: D

Question #126

An application running on Amazon EC2 instances must access objects within an Amaon S3 busket that are encrypted using server-side encryption using AWS

KMS encryption keys (SSE-KMS). The application must have access to the customer master key (CMK) to decrypt the objects.

Which combination of steps will grant the application access? (Select TWO.)

- A. Write an S3 bucket policy that grants the bucket access to the key.
- B. Grant access to the key in the IAM EC2 role attached to the application's EC2 instances.
- C. Write a key policy that enables IAM policies to grant access to the key.
- D. Grant access to the key in the S3 bucket's ACL
- E. Create a Systems Manager parameter that exposes the KMS key to the EC2 instances. AE

Answer: BE

Question #127

A company needs a fully-managed source control service that will work in AWS. The service must ensure that revision control synchronizes multiple distributed repositories by exchanging sets of changes peer-to-peer. All users need to work productively even when not connected to a network.

Which source control service should be used?

- A. Subversion
- B. AWS CodeBuild
- C. AWS CodeCommit
- D. AWS CodeStar

Answer: C

Question #128

<https://itexamcertified.com>

<https://itexamcertified.com>

A Developer is writing a serverless application that requires that an AWS Lambda function be invoked every 10 minutes.

What is an automated and serverless way to trigger the function?

- A. Deploy an Amazon EC2 instance based on Linux, and edit its /etc/crontab file by adding a command to periodically invoke the Lambda function.
- B. Configure an environment variable named PERIOD for the Lambda function. Set the value to 600.
- C. Create an Amazon CloudWatch Events rule that triggers on a regular schedule to invoke the Lambda function.
- D. Create an Amazon SNS topic that has a subscription to the Lambda function with a 600-second timer.

Answer: C

Reference:

<https://aws.amazon.com/blogs/architecture/a-serverless-solution-for-invoking-aws-lambda-at-a-sub-minute-frequency/>

Question #129

A Developer is writing an imaging micro service on AWS Lambda. The service is dependent on several libraries that are not available in the Lambda runtime environment.

Which strategy should the Developer follow to create the Lambda deployment package?

- A. Create a ZIP file with the source code and all dependent libraries.
- B. Create a ZIP file with the source code and a script that installs the dependent libraries at runtime.
- C. Create a ZIP file with the source code. Stage the dependent libraries on an Amazon S3 bucket indicated by the Lambda environment variable LD_LIBRARY_PATH
- D. Create a ZIP file with the source code and a buildspec.yaml file that installs the dependent libraries on AWS Lambda.

Answer: A

Question #130

A Developer is designing a fault-tolerant environment where client sessions will be saved.

How can the Developer ensure that no sessions are lost if an Amazon EC2 instance fails?

- A. Use sticky sessions with an Elastic Load Balancer target group.
- B. Use Amazon SQS to save session data.
- C. Use Amazon DynamoDB to perform scalable session hadling.

<https://itexamcertified.com>

<https://itexamcertified.com>

- D. Use Elastic Load Balancer connection draining to stop sending requests to failing instances.

Answer: A

Question #131

In a move toward using microservices, a company's Management team has asked all Development teams to build their services so that API requests depend only on that service's data store. One team is building a Payments service which has its own database; the service needs data that originates in the Accounts database. Both are using Amazon DynamoDB.

What approach will result in the simplest, decoupled, and reliable method to get near-real time updates from the Accounts database?

- A. Use Amazon Glue to perform frequent ETL updates from the Accounts database to the Payments database.
- B. Use Amazon ElastiCache in Payments, with the cache updated by triggers in the Accounts database.
- C. Use Amazon Kinesis Data Firehouse to deliver all changes from the Accounts database to the Payments database.
- D. Use Amazon DynamoDB Streams to deliver all changes from the Accounts database to the Payments database.

Answer: D

Reference:

<https://aws.amazon.com/blogs/database/how-to-perform-ordered-data-replication-between-applications-by-using-amazon-dynamodb-streams/>

Question #132

How should custom libraries be utilized in AWS Lambda?

- A. Host the library on Amazon S3 and reference to it from the Lambda function.
- B. Install the library locally and upload a ZIP file of the Lambda function.
- C. Import the necessary Lambda blueprint when creating the function.
- D. Modify the function runtime to include the necessary library.

Answer: D

Reference:

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

<https://itexamcertified.com>

Question #133

A company needs to secure its existing website running behind an Elastic Load Balancer. The website's Amazon EC2 instances are CPU-constrained.

What should be done to secure the website while not increasing the CPU load on the EC2 web servers? (Select TWO.)

- A. Configure an Elastic Load Balancer with SSL pass-through.
- B. Configure SSL certificates on an Elastic Load Balancer.
- C. Configure an Elastic Load Balancer with a Loadable Storage System.
- D. Install SSL certificates on the EC2 instances.
- E. Configure an Elastic Load Balancer with SSL termination.

Answer: BE

Question #134

An AWS Lambda function generates a 3MB JSON file and then uploads it to an Amazon S3 bucket daily. The file contains sensitive information, so the Developer must ensure that it is encrypted before uploading to the bucket.

Which of the following modifications should the Developer make to ensure that the data is encrypted before uploading it to the bucket?

- A. Use the default AWS KMS customer master key for S3 in the Lambda function code.
- B. Use the S3 managed key and call the GenerateDataKey API to encrypt the file.
- C. Use the GenerateDataKey API, then use that data key to encrypt the file in the Lambda function code.
- D. Use a custom KMS customer master key created for S3 in the Lambda function code.

Answer: C

Question #135

A Developer wants to find a list of items in a global secondary index from an Amazon DynamoDB table.

Which DynamoDB API call can the Developer use in order to consume the LEAST number of read capacity units?

- A. Scan operation using eventually-consistent reads
- B. Query operation using strongly-consistent reads
- C. Query operation using eventually-consistent reads
- D. Scan operation using strongly-consistent reads

<https://itexamcertified.com>

Answer: C

Question #136

A Developer has published an update to an application that is served to a global user base using Amazon CloudFront. After deploying the application, users are not able to see the updated changes.

How can the Developer resolve this issue?

- A. Remove the origin from the CloudFront configuration and add it again.
- B. Disable forwarding of query strings and request headers from the CloudFront distribution configuration.
- C. Invalidate all the application objects from the edge caches.
- D. Disable the CloudFront distribution and enable it again to update all the edge locations.

Answer: C

Question #137

A Developer must deploy a new AWS Lambda function using an AWS CloudFormation template.

Which procedures will deploy a Lambda function? (Select TWO.)

- A. Upload the code to an AWS CodeCommit repository, then add a reference to it in an AWS::Lambda::Function resource in the template.
- B. Create an AWS::Lambda::Function resource in the template, then write the code directly inside the CloudFormation template.
- C. Upload a .ZIP file containing the function code to Amazon S3, then add a reference to it in an AWS::Lambda::Function resource in the template.
- D. Upload a .ZIP file to AWS CloudFormation containing the function code, then add a reference to it in an AWS::Lambda::Function resource in the template.
- E. Upload the function code to a private Git repository, then add a reference to it in an AWS::Lambda::Function resource in the template.

Answer: Explanation

Question #138

A Developer wants to enable AWS X-Ray for a secure application that runs in an Amazon ECS environment.

What combination of steps will enable X-Ray? (Select THREE.)

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Create a Docker image that runs the X-Ray daemon.
- B. Add instrumentation to the application code for X-Ray.
- C. Install the X-Ray daemon on the underlying EC2 instance.
- D. Configure and use an IAM EC2 instance role.
- E. Register the application with X-Ray.
- F. Configure and use an IAM role for tasks.

Answer: ABF

Reference:

<https://aws.amazon.com/blogs/aws/category/aws-x-ray/>

Question #139

A Developer is designing a new application that uses Amazon S3. To satisfy compliance requirements, the Developer must encrypt the data at rest.

How can the Developer accomplish this?

- A. Use s3:x-amz-acl as a condition in the S3 bucket policy.
- B. Use Amazon RDS with default encryption.
- C. Use aws:SecureTransport as a condition in the S3 bucket policy.
- D. Turn on S3 default encryption for the S3 bucket.

Answer: D

Question #140

An AWS Elastic Beanstalk application needs to be deployed in multiple regions and requires a different Amazon Machine Image (AMI) in each region.

Which AWS CloudFormation template key can be used to specify the correct AMI for each region?

- A. Parameters
- B. Outputs
- C. Mappings
- D. Resources

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: C

Reference:

<https://docs.aws.amazon.com/marketplace/latest/userguide/clouformation.html>

Question #141

A Developer has been asked to make changes to the source code of an AWS Lambda function. The function is managed using an AWS CloudFormation template. The template is configured to load the source code from an Amazon S3 bucket. The Developer manually created a .ZIP file deployment package containing the changes and put the file into the correct location on Amazon S3. When the function is invoked, the code changes have not been applied.

What step is required to update the function with the changes?

- A. Delete the .ZIP file on S3, and re-upload by using a different object key name.
- B. Update the CloudFormation stack with the correct values for the function code properties S3Bucket, S3Key, or S3ObjectVersion.
- C. Ensure that the function source code is base64-encoded before uploading the deployment package to S3.
- D. Modify the execution role of the Lambda function to allow S3 access permission to the deployment package .ZIP file.

Answer: B

Question #142

A Developer needs to design an application running on AWS that will be used to consume Amazon SQS messages that range from 1 KB up to 1GB in size.

How should the Amazon SQS messages be managed?

- A. Use Amazon S3 and the Amazon SQS CLI.
- B. Use Amazon S3 and the Amazon SQS Extended Client Library for Java.
- C. Use Amazon EBS and the Amazon SQS CLI.
- D. Use Amazon EFS and the Amazon SQS CLI.

Answer: A

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-limits.html>

<https://itexamcertified.com>

Question #143

A company is developing an application that will run on several Amazon EC2 instances in an Auto Scaling group and can access a database running on Amazon

EC2. The application needs to store secrets required to connect to the database. The application must allow for periodic secret rotation, and there should be no changes to the application when a secret changes.

What is the SAFEST way to meet these requirements?

- A. Associate an IAM role to the EC2 instance where the application is running with permission to access the database.
- B. Use AWS Systems Manager Parameter Store with the SecureString data type to store secrets.
- C. Configure the application to store secrets in Amazon S3 object metadata.
- D. Hard code the database secrets in the application code itself. A

Answer: B

Question #144

A Developer writes an AWS Lambda function and uploads the code in a .ZIP file to Amazon S3. The Developer makes changes to the code and uploads a new

.ZIP file to Amazon S3. However, Lambda executes the earlier code.

How can the Developer fix this in the LEAST disruptive way?

- A. Create another Lambda function and specify the new .ZIP file.
- B. Call the update-function-code API.
- C. Remove the earlier .ZIP file first, then add the new .ZIP file.
- D. Call the create-alias API. B

Answer: B

Question #145

An AWS Lambda function must read data from an Amazon RDS MySQL database in a VPC and also reach a public endpoint over the internet to get additional data.

Which steps must be taken to allow the function to access both the RDS resource and the public endpoint? (Select TWO.)

- A. Modify the default configuration for the Lambda function to associate it with an Amazon VPC private subnet.
- B. Modify the default network access control list to allow outbound traffic.

<https://itexamcertified.com>

- C. Add a NAT Gateway to the VPC.
- D. Modify the default configuration of the Lambda function to associate it with a VPC public subnet.
- E. Add an environmental variable to the Lambda function to allow outbound internet access.

Answer: AC

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/vpc.html>

Question #146

A Developer must build an application that uses Amazon DynamoDB. The requirements state that items being stored in the DynamoDB table will be 7KB in size and that reads must be strongly consistent. The maximum read rate is 3 items per second, and the maximum write rate is 10 items per second.

How should the Developer size the DynamoDB table to meet these requirements?

- A. Read: 3 read capacity units Write: 70 write capacity units
- B. Read: 6 read capacity units Write: 70 write capacity units
- C. Read: 6 read capacity units Write: 10 write capacity units
- D. Read: 3 read capacity units Write: 10 write capacity units

Answer: B

Question #147

A Developer is creating an AWS Lambda function to process a stream of data from an Amazon Kinesis Data Stream. When the Lambda function parses the data and encounters a missing field, it exits the function with an error. The function is generating duplicate records from the Kinesis stream. When the Developer looks at the stream output without the Lambda function, there are no duplicate records.

What is the reason for the duplicates?

- A. The Lambda function did not advance the Kinesis stream pointer to the next record after the error.
- B. The Lambda event source used asynchronous invocation, resulting in duplicate records.
- C. The Lambda function did not handle the error, and the Lambda service attempted to reprocess the data.
- D. The Lambda function is not keeping up with the amount of data coming from the stream.

Answer: C

<https://itexamcertified.com>

Question #148

A company maintains an application responsible for processing several thousand external callbacks each day. The company's System administrators want to know how many callbacks are being received on a rolling basis, and they want this data available for 10 days.

The company also wants the ability to issue automated alerts if the number of callbacks exceeds the defined thresholds.

What is the MOST cost-effective way to address the need to track and alert on these statistics?

- A. Push callback data to an Amazon RDS database that can be queried to show historical data and to alert on exceeded thresholds.
- B. Push callback data to AWS X-Ray and use AWS Lambda to query, display, and alert on exceeded thresholds.
- C. Push callback data to Amazon Kinesis Data Streams and invoke an AWS Lambda function that stores data in Amazon DynamoDB and sends the required alerts.
- D. Push callback data to Amazon CloudWatch as a custom metric and use the CloudWatch alerting mechanisms to alert System Administrators. C

Answer: D

Question #149

A company has a website that is developed in PHP and WordPress and is launched using AWS Elastic Beanstalk. There is a new version of the website that needs to be deployed in the Elastic Beanstalk environment. The company cannot tolerate having the website offline if an update fails. Deployments must have minimal impact and rollback as soon as possible.

What deployment method should be used?

- A. All at once
- B. Rolling
- C. Snapshots
- D. Immutable

Answer: D

Question #150

A company has a multi-tiered web application on AWS. During a recent spike in traffic, one of the primary relational databases on Amazon RDS could not serve all the traffic. Some read queries for repeatedly accessed items failed, so users received error messages.

<https://itexamcertified.com>

What can be done to minimize the impact on database read queries MOST efficiently during future traffic spikes?

- A. Use Amazon S3 to cache database query results.
- B. Use Amazon RDS as a custom origin for Amazon CloudFront.
- C. Use local storage and memory on Amazon EC2 instances to cache data.
- D. Use Amazon ElastiCache in front of the primary database to cache data.

Answer: D

Question #151

A Development team currently supports an application that uses an in-memory store to save accumulated game results. Individual results are stored in a database. As part of migrating to AWS, the team needs to use automatic scaling. The team knows this will yield inconsistent results.

Where should the team store these accumulated game results to BEST allow for consistent results without impacting performance?

- A. Amazon S3
- B. Amazon RDS
- C. Amazon ElastiCache
- D. Amazon Kinesis C

Answer: C

Question #152

In a multi-container Docker environment in AWS Elastic Beanstalk, what is required to configure container instances in the environment?

- A. An Amazon ECS task definition
- B. An Amazon ECS cluster
- C. A Docker in an application package
- D. A CLI for Elastic Beanstalk

Answer: B

Reference:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker_ecs.html

<https://itexamcertified.com>

Question #153

An application that runs on an Amazon EC2 instance needs to access and make API calls to multiple AWS services.

What is the MOST secure way to provide access to the AWS services with MINIMAL management overhead?

- A. Use AWS KMS to store and retrieve credentials.
- B. Use EC2 instance profiles.
- C. Use AWS root user to make requests to the application.
- D. Store and retrieve credentials from AWS CodeCommit.

Answer: B

Question #154

A company is creating an application that will require users to access AWS services and allow them to reset their own passwords.

Which of the following would allow the company to manage users and authorization while allowing users to reset their own passwords?

- A. Amazon Cognito identity pools and AWS STS
- B. Amazon Cognito identity pools and AWS IAM
- C. Amazon Cognito user pools and AWS KMS
- D. Amazon Cognito user pools and identity pools

Answer: D

Question #155

A company has three different environments: Development, QA, and Production. The company wants to deploy its code first in the Development environment, then QA, and then Production.

Which AWS service can be used to meet this requirement?

- A. Use AWS CodeCommit to create multiple repositories to deploy the application.
- B. Use AWS CodeBuild to create, configure, and deploy multiple build application projects.
- C. Use AWS Data Pipeline to create multiple data pipeline provisions to deploy the application.
- D. Use AWS CodeDeploy to create multiple deployment groups. C

<https://itexamcertified.com>

Answer: D

Question #156

A company uses Amazon DynamoDB for managing and tracking orders. The DynamoDB table is partitioned based on the order date. The company receives a huge increase in orders during a sales event, causing DynamoDB writes to throttle, and the consumed throughput is far below the provisioned throughput.

According to AWS best practices, how can this issue be resolved with MINIMAL costs?

- A. Create a new DynamoDB table for every order date.
- B. Increase the read and write capacity units of the DynamoDB table.
- C. Add a random number suffix to the partition key values.
- D. Add a global secondary index to the DynamoDB table.

Answer: C

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/throttled-ddb/>

Question #157

A company is providing services to many downstream consumers. Each consumer may connect to one or more services. This has resulted in a complex architecture that is difficult to manage and does not scale well. The company needs a single interface to manage these services to consumers.

Which AWS service should be used to refactor this architecture?

- A. AWS Lambda
- B. AWS X-Ray
- C. Amazon SQS
- D. Amazon API Gateway

Answer: D

Question #158

A Developer is creating a serverless website with content that includes HTML files, images, videos, and JavaScript (client-side scripts).

Which combination of services should the Developer use to create the website?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Amazon S3 and Amazon CloudFront
- B. Amazon EC2 and Amazon ElastiCache
- C. Amazon ECS and Redis
- D. AWS Lambda and Amazon API Gateway

Answer: A

Reference:

<https://d1.awsstatic.com/whitepapers/Building%20Static%20Websites%20on%20AWS.pdf>

Question #159

A Development team has pushed out 10 applications running on several Amazon EC2 instances. The Operations team is asking for a graphical representation of one key performance metric for each application. These metrics should be available on one screen for easy monitoring.

Which steps should the Developer take to accomplish this using Amazon CloudWatch?

- A. Create a custom namespace with a unique metric name for each application.
- B. Create a custom dimension with a unique metric name for each application.
- C. Create a custom event with a unique metric name for each application.
- D. Create a custom alarm with a unique metric name for each application.

Answer: A

Reference:

<http://jayendrapatil.com/tag/cloudwatch/>

Question #160

A Developer wants access to make the log data of an application running on an EC2 instance available to systems administrators.

Which of the following enables monitoring of this metric in Amazon CloudWatch?

- A. Retrieve the log data from CloudWatch using the GetMetricData API call
- B. Retrieve the log data from AWS CloudTrail using the LookupEvents API call.
- C. Launch a new EC2 instance, configure Amazon CloudWatch Events, and then install the application.
- D. Install the Amazon CloudWatch Logs agent on the EC2 instance that the application is running on.

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: D

Question #161

A nightly batch job loads 1 million new records into a DynamoDB table. The records are only needed for one hour, and the table needs to be empty by the next night's batch job.

Which is the MOST efficient and cost-effective method to provide an empty table?

- A. Use DeleteItem using a ConditionExpression.
- B. Use BatchWriteItem to empty all of the rows.
- C. Write a recursive function that scans and calls out DeleteItem.
- D. Create and then delete the table after the task has completed.

Answer: D

Question #162

A company has an application that logs all information to Amazon S3. Whenever there is a new log file, an AWS Lambda function is invoked to process the log files. The code works, gathering all of the necessary information. However, when checking the Lambda function logs, duplicate entries with the same request ID are found.

What is causing the duplicate entries?

- A. The S3 bucket name was specified incorrectly.
- B. The Lambda function failed, and the Lambda service retired the invocation with a delay.
- C. There was an S3 outage, which caused duplicate entries of the sale log file.
- D. The application stopped intermittently and then resumed.

Answer: B

Question #163

A company maintains a REST service using Amazon API Gateway and the API Gateway native API key validation. The company recently launched a new registration page, which allows users to sign up for the service. The registration page creates a new API key using CreateApiKey and sends the new key to the user. When the user attempts to call the API using this key, the user receives a 403 Forbidden error. Existing users are unaffected and can still call the API.

What code updates will grant these new users access to the API?

- A. The createDeployment method must be called so the API can be redeployed to include the newly created API key.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. The updateAuthorizer method must be called to update the API's authorizer to include the newly created API key.
- C. The importApiKeys method must be called to import all newly created API keys into the current stage of the API.
- D. The createUsagePlanKey method must be called to associate the newly created API key with the correct usage plan.

Answer: D

Question #164

A Developer is writing a mobile application that allows users to view images from an S3 bucket. The users must be able to log in with their Amazon login, as well as Facebook® and/or Google® accounts.

How can the Developer provide this authentication functionality?

- A. Use Amazon Cognito with web identity federation.
- B. Use Amazon Cognito with SAML-based identity federation.
- C. Use AWS IAM Access/Secret keys in the application code to allow Get* on the S3 bucket.
- D. Use AWS STS AssumeRole in the application code and assume a role with Get* permissions on the S3 bucket.

Answer: A

Reference:

<http://jayendrapatil.com/tag/iam-role/>

Question #165

A Developer has created a Lambda function and is finding that the function is taking longer to complete than expected. After some debugging, the Developer has discovered that increasing compute capacity would improve performance.

How can the Developer increase the Lambda compute resources?

- A. Run on a larger instance size with more compute capacity.
- B. Increase the maximum execution time.
- C. Specify a larger compute capacity when calling the Lambda function.
- D. Increase the allocated memory for the Lambda function.

Answer: D

<https://itexamcertified.com>

Question #166

An e-commerce site allows returning users to log in to display customized web pages. The workflow is shown in the image below:



An application is running on EC2 instances. Amazon RDS is used for the database that stores user accounts and preferences. The website freezes or is slow to load while waiting for the login step to complete. The remaining components of the site are well-optimized.

Which of the following techniques will resolve this issue? (Select Two.)

- A. Implement the user login page as an asynchronous Lambda function.
- B. Use Amazon ElastiCache for MemCached to cache user data.
- C. Use Amazon Application Load Balancer to load balance the traffic to the website.
- D. Call the database asynchronously so the code can continue executing.
- E. Batch login requests from hundreds of users together as a single read request to the database. BD

Answer: BD

Question #167

A Developer is building a mobile application and needs any update to user profile data to be pushed to all devices accessing the specific identity. The Developer does not want to manage a back end to maintain the user profile data.

<https://itexamcertified.com>

What is the MOST efficient way for the Developer to achieve these requirements using Amazon Cognito?

- A. Use Cognito federated identities.
- B. Use a Cognito user pool.
- C. Use Cognito Sync.
- D. Use Cognito events.

Answer: C

Question #168

A company is migrating a single-server, on-premises web application to AWS. The company intends to use multiple servers behind an Elastic Load Balancer

(ELB) to balance the load, and will also store session data in memory on the web server. The company does not want to lose that session data if a server fails or goes offline, and it wants to minimize user's downtime.

Where should the company move session data to MOST effectively reduce downtime and make users' session data more fault tolerant?

- A. An Amazon ElastiCache for Redis cluster
- B. A second Amazon EBS volume
- C. The web server's primary disk
- D. An Amazon EC2 instance dedicated to session data

Answer: A

Question #169

A Developer created configuration specifications for an AWS Elastic Beanstalk application in a file named healthcheckurl.yaml in the .ebextensions/directory of their application source bundle. The file contains the following:

```
option_settings:  
  - namespace: aws:elasticbeanstalk:application  
    option_name: Application Healthcheck URL  
    value: /health_check
```

After the application launches, the health check is not being run on the correct path, even though it is valid.

What can be done to correct this configuration file?

- A. Convert the file to JSON format.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Rename the file to a .config extension.
- C. Change the configuration section from options_settings to resources.
- D. Change the namespace of the option settings to a custom namespace.

Answer: B

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/ebextensions.html>

Question #170

A Developer is making changes to a custom application that is currently using AWS Elastic Beanstalk.

After the Developer completes the changes, what solutions will update the Elastic Beanstalk environment with the new application version? (Choose two.)

- A. Package the application code into a .zip file, and upload, then deploy the packaged application from the AWS Management Console
- B. Package the application code into a .tar file, create a new application version from the AWS Management Console, then update the environment by using AWS CLI
- C. Package the application code into a .tar file, and upload and deploy the packaged application from the AWS Management Console
- D. Package the application code into a .zip file, create a new application version from the packaged application by using AWS CLI, then update the environment by using AWS CLI
- E. Package the application code into a .zip file, create a new application version from the AWS Management Console, then rebuild the environment by using AWS CLI

Answer:AD

Question #171

To include objects defined by the AWS Serverless Application Model (SAM) in an AWS CloudFormation template, in addition to Resources, what section MUST be included in the document root?

- A. Conditions
- B. Globals
- C. Transform
- D. Properties

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: C

Reference:

<https://docs.aws.amazon.com/cloud9/latest/user-guide/lambda-functions.html>

Question #172

A company is using Amazon RDS MySQL instances for its application database tier and Apache Tomcat servers for its web tier. Most of the database queries from web applications are repeated read requests.

Use of which AWS service would increase in performance by adding in-memory store for repeated read queries?

- A. Amazon RDS Multi-AZ
- B. Amazon SQS
- C. Amazon ElastiCache
- D. Amazon RDS read replica

Answer: C

Question #173

A Developer is investigating an issue whereby certain requests are passing through an Amazon API Gateway endpoint /MyAPI, but the requests do not reach the

AWS Lambda function backing /MyAPI. The Developer found that a second Lambda function sometimes runs at maximum concurrency allowed for the given AWS account.

How can the Developer address this issue?

- A. Manually reduce the concurrent execution limit at the account level
- B. Add another API Gateway stage for /MyAPI, and shard the requests
- C. Configure the second Lambda function's concurrency execution limit
- D. Reduce the throttling limits in the API Gateway /MyAPI endpoint C

Answer: C

Question #174

A Developer must analyze performance issues with production-distributed applications written as AWS Lambda functions. These distributed Lambda applications invoke other components that make up the applications.

How should the Developer identify and troubleshoot the root cause of the performance issues in production?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Add logging statements to the Lambda functions, then use Amazon CloudWatch to view the logs.
- B. Use AWS Cloud Trail and then examine the logs
- C. Use AWS X-Ray, then examine the segments and errors
- D. Run Amazon Inspector agents and then analyze performance

Answer: C

Question #175

A Developer wants to debug an application by searching and filtering log data. The application logs are stored in Amazon CloudWatch Logs. The Developer creates a new metric filter to count exceptions in the application logs. However, no results are returned from the logs.

What is the reason that no filtered results are being returned?

- A. A setup of the Amazon CloudWatch interface VPC endpoint is required for filtering the CloudWatch Logs in the VPC
- B. CloudWatch Logs only publishes metric data for events that happen after the filter is created
- C. The log group for CloudWatch Logs should be first streamed to Amazon Elasticsearch Service before metric filtering returns the results
- D. Metric data points for logs groups can be filtered only after they are exported to an Amazon S3 bucket

Answer: B

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringLogData.html>

Question #176

An e-commerce web application that shares session state on-premises is being migrated to AWS. The application must be fault tolerant, natively highly scalable, and any service interruption should not affect the user experience.

What is the best option to store the session state?

- A. Store the session state in Amazon ElastiCache
- B. Store the session state in Amazon CloudFront
- C. Store the session state in Amazon S3
- D. Enable session stickiness using elastic load balancers

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: A

Question #177

A Developer is creating a template that uses AWS CloudFormation to deploy an application. This application is serverless and uses Amazon API Gateway,

Amazon DynamoDB, and AWS Lambda.

Which tool should the Developer use to define simplified syntax for expressing serverless resources?

- A. CloudFormation serverless intrinsic functions
- B. AWS serverless express
- C. An AWS serverless application model
- D. A CloudFormation serverless plugin

Answer: C

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-application-fundamentals.html>

Question #178

A Developer has a stateful web server on-premises that is being migrated to AWS. The Developer must have greater elasticity in the new design.

How should the Developer re-factor the application to make it more elastic? (Choose two.)

- A. Use pessimistic concurrency on Amazon DynamoDB
- B. Use Amazon CloudFront with an Auto Scaling group
- C. Use Amazon CloudFront with an AWS Web Application Firewall
- D. Store session state data in an Amazon DynamoDB table
- E. Use an ELB with an Auto Scaling group

Answer: DE

Question #179

A company needs to distribute firmware updates to its customers around the world.

Which service will allow easy and secure control of the access to the downloads at the lowest cost?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Use Amazon CloudFront with signed URLs for Amazon S3
- B. Create a dedicated Amazon CloudFront Distribution for each customer
- C. Use Amazon CloudFront with AWS Lambda@Edge
- D. Use Amazon API Gateway and AWS Lambda to control access to an S3 bucket

Answer: A

Question #180

A company is running an application built on AWS Lambda functions. One Lambda function has performance issues when it has to download a 50MB file from the

Internet in every execution. This function is called multiple times a second.

What solution would give the BEST performance increase?

- A. Cache the file in the /tmp directory
- B. Increase the Lambda maximum execution time
- C. Put an Elastic Load Balancer in front of the Lambda function
- D. Cache the file in Amazon S3 D

Answer: A

Question #181

An application writes items to an Amazon DynamoDB table. As the application scales to thousands of instances, calls to the DynamoDB API generate occasional

ThrottlingException errors. The application is coded in a language incompatible with the AWS SDK.

How should the error be handled?

- A. Add exponential backoff to the application logic
- B. Use Amazon SQS as an API message bus
- C. Pass API calls through Amazon API Gateway
- D. Send the items to DynamoDB through Amazon Kinesis Data Firehose

Answer: A

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Programming.Errors.html>

Question #182

An application deployed on AWS Elastic Beanstalk experiences increased error rates during deployments of new application versions, resulting in service degradation for users. The Development team believes that this is because of the reduction in capacity during the deployment steps. The team would like to change the deployment policy configuration of the environment to an option that maintains full capacity during deployment while using the existing instances.

Which deployment policy will meet these requirements while using the existing instances?

- A. All at once
- B. Rolling
- C. Rolling with additional batch
- D. Immutable

Answer: C

Reference:

<https://aws.amazon.com/blogs/developer/version-2-of-the-aws-elastic-beanstalk-windows-server-platform/>

Question #183

A Developer is working on an application that handles 10MB documents that contain highly-sensitive data. The application will use AWS KMS to perform client-side encryption.

What steps must be followed?

- A. Invoke the Encrypt API passing the plaintext data that must be encrypted, then reference the customer managed key ARN in the KeyId parameter
- B. Invoke the GenerateRandom API to get a data encryption key, then use the data encryption key to encrypt the data
- C. Invoke the GenerateDataKey API to retrieve the encrypted version of the data encryption key to encrypt the data
- D. Invoke the GenerateDataKey API to retrieve the plaintext version of the data encryption key to encrypt the data

Answer: D

Question #184

<https://itexamcertified.com>

A Developer is building a web application that uses Amazon API Gateway to expose an AWS Lambda function to process requests from clients. During testing, the Developer notices that the API Gateway times out even though the Lambda function finishes under the set time limit.

Which of the following API Gateway metrics in Amazon CloudWatch can help the Developer troubleshoot the issue? (Choose two.)

- A. CacheHitCount
- B. IntegrationLatency
- C. CacheMissCount
- D. Latency
- E. Count

Answer: BD

Question #185

An AWS Lambda function must access an external site by using a regularly rotated user name and password. These items must be kept securely and cannot be stored in the function code.

What combination of AWS services can be used to accomplish this? (Choose two.)

- A. AWS Certificate Manager (ACM)
- B. AWS Systems Manager Parameter Store
- C. AWS Trusted Advisor
- D. AWS KMS
- E. Amazon GuardDuty

Answer: BD

Question #186

A Developer is trying to deploy a serverless application using AWS CodeDeploy. The application was updated and needs to be redeployed.

What file does the Developer need to update to push that change through CodeDeploy?

- A. dockerrun.aws.json
- B. buildspec.yml
- C. appspec.yml

<https://itexamcertified.com>

D. ebextensions.config

Answer: C

Question #187

A Developer wants to upload data to Amazon S3 and must encrypt the data in transit.

Which of the following solutions will accomplish this task? (Choose two.)

- A. Set up hardware VPN tunnels to a VPC and access S3 through a VPC endpoint
- B. Set up Client-Side Encryption with an AWS KMS-Managed Customer Master Key
- C. Set up Server-Side Encryption with AWS KMS-Managed Keys
- D. Transfer the data over an SSL connection
- E. Set up Server-Side Encryption with S3-Managed Keys

Answer: BD

Question #188

A company is running a Docker application on Amazon ECS. The application must scale based on user load in the last 15 seconds.

How should a Developer instrument the code so that the requirement can be met?

- A. Create a high-resolution custom Amazon CloudWatch metric for user activity data, then publish data every 30 seconds
- B. Create a high-resolution custom Amazon CloudWatch metric for user activity data, then publish data every 5 seconds
- C. Create a standard-resolution custom Amazon CloudWatch metric for user activity data, then publish data every 30 seconds
- D. Create a standard-resolution custom Amazon CloudWatch metric for user activity data, then publish data every 5 seconds

Answer: B

Question #189

<https://itexamcertified.com>

<https://itexamcertified.com>

A company needs to ingest terabytes of data each hour from thousands of sources that are delivered almost continually throughout the day. The volume of messages generated varies over the course of the day. Messages must be delivered in real time for fraud detection and live operational dashboards.

Which approach will meet these requirements?

- A. Send the messages to an Amazon SQS queue, then process the messages by using a fleet of Amazon EC2 instances
- B. Use the Amazon S3 API to write messages to an S3 bucket, then process the messages by using Amazon Redshift
- C. Use AWS Data Pipeline to automate the movement and transformation of data
- D. Use Amazon Kinesis Data Streams with Kinesis Client Library to ingest and deliver messages

Answer: D

Reference:

<https://noise.getoto.net/tag/amazon-kinesis-analytics/>

Question #190

A Developer accesses AWS CodeCommit over SSH. The SSH keys configured to access AWS CodeCommit are tied to

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "codecommit:BatchGetRepositories",  
                "codecommit:Get*",  
                "codecommit>List*",  
                "codecommit:GitPull"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

a user with the following permissions:

<https://itexamcertified.com>

<https://itexamcertified.com>

The Developer needs to create/delete branches.

Which specific IAM permissions need to be added, based on the principle of least privilege?

- A. "codecommit:CreateBranch" "codecommit:DeleteBranch"
- B. "codecommit:Put*"
- C. "codecommit:Update*"
- D. "codecommit:/*"

Answer: A

Question #191

A Developer has been asked to create an AWS Lambda function that is triggered any time updates are made to items in an Amazon DynamoDB table. The function has been created, and appropriate permissions have been added to the Lambda execution role. Amazon DynamoDB streams have been enabled for the table, but the function is still not being triggered.

Which option would enable DynamoDB table updates to trigger the Lambda function?

- A. Change the StreamViewType parameter value to NEW_AND_OLD_IMAGES for the DynamoDB table
- B. Configure event source mapping for the Lambda function
- C. Map an Amazon SNS topic to the DynamoDB streams
- D. increase the maximum execution time (timeout) setting of the Lambda function

Answer: B

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/with-ddb.html>

Question #192

An application is being developed to audit several AWS accounts. The application will run in Account A and must access AWS services in Accounts B and C.

What is the MOST secure way to allow the application to call AWS services in each audited account?

- A. Configure cross-account roles in each audited account. Write code in Account a that assumes those roles
- B. Use S3 cross-region replication to communicate among accounts, with Amazon S3 event notifications to trigger Lambda functions
- C. Deploy an application in each audited account with its own role. Have Account A authenticate with the application

<https://itexamcertified.com>

<https://itexamcertified.com>

D. Create an IAM user with an access key in each audited account. Write code in Account A that uses those access keys

Answer: A

Question #193

A Developer is building a three-tier web application that should be able to handle a minimum of 5000 requests per minute. Requirements state that the web tier should be completely stateless while the application maintains session state for the users.

How can session data be externalized, keeping latency at the LOWEST possible value?

- A. Create an Amazon RDS instance, then implement session handling at the application level to leverage a database inside the RDS database instance for session data storage
- B. Implement a shared file system solution across the underlying Amazon EC2 instances, then implement session handling at the application level to leverage the shared file system for session data storage
- C. Create an Amazon ElastiCache Memcached cluster, then implement session handling at the application level to leverage the cluster for session data storage
- D. Create an Amazon DynamoDB table, then implement session handling at the application level to leverage the table for session data storage

Answer: C

<https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug>SelectEngine.html>

Question #194

An Amazon DynamoDB table uses a Global Secondary Index (GSI) to support read queries. The primary table is write-heavy, whereas the GSI is used for read operations. Looking at Amazon CloudWatch metrics, the Developer notices that write operations to the primary table are throttled frequently under heavy write activity. However, write capacity units to the primary table are available and not fully consumed.

Why is the table being throttled?

- A. The GSI write capacity units are underprovisioned
- B. There are not enough read capacity units on the primary table
- C. Amazon DynamoDB Streams is not enabled on the table
- D. A large write operation is being performed against another table D

Answer: A

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #195

A company runs an e-commerce website that uses Amazon DynamoDB where pricing for items is dynamically updated in real time. At any given time, multiple updates may occur simultaneously for pricing information on a particular product. This is causing the original editor's changes to be overwritten without a proper review process.

Which DynamoDB write option should be selected to prevent this overwriting?

- A. Concurrent writes
- B. Conditional writes
- C. Atomic writes
- D. Batch writes B

Answer: B

Question #196

A company needs a version control system for collaborative software development. Features of the system must include the following:

- ➡ Support for batches of changes across multiple files
- ➡ Parallel branching
- ➡ Version tracking

Which AWS service will meet these requirements?

- A. AWS CodePipeline
- B. Amazon S3
- C. AWS Code Build
- D. AWS CodeCommit D

Answer: D

Reference:

<https://docs.aws.amazon.com/codecommit/latest/userguide/welcome.html>

Question #197

A company is using continuous integration and continuous delivery systems. A Developer now needs to automate a software package deployment to both

Amazon EC2 instances and virtual servers running on-premises.

<https://itexamcertified.com>

<https://itexamcertified.com>

Which AWS service should be used to accomplish this?

- A. AWS CodePipeline
- B. AWS CodeBuild
- C. AWS Elastic Beanstalk
- D. AWS CodeDeploy

Answer: D

Question #198

A Developer created a new AWS account and must create a scalable AWS Lambda function that meets the following requirements for concurrent execution:

- ➡ Average execution time of 100 seconds
- ➡ 50 requests per second

Which step must be taken prior to deployment to prevent errors?

- A. Implement dead-letter queues to capture invocation errors
- B. Add an event source from Amazon API Gateway to the Lambda function
- C. Implement error handling within the application code
- D. Contact AWS Support to increase the concurrent execution limits

Answer: D

Question #199

A Development team wants to instrument their code to provide more detailed information to AWS X-Ray than simple outgoing and incoming requests. This will generate large amounts of data, so the Development team wants to implement indexing so they can filter the data.

What should the Development team do to achieve this?

- A. Add annotations to the segment document and the code
- B. Add metadata to the segment document and the code
- C. Configure the necessary X-Ray environment variables
- D. Install required plugins for the appropriate AWS SDK A

Answer: A

<https://itexamcertified.com>

<https://itexamcertified.com>

Reference:

<https://docs.aws.amazon.com/xray/latest/devguide/xray-concepts.html>

Question #200

A team of Developers must migrate an application running inside an AWS Elastic Beanstalk environment from a Classic Load Balancer to an Application Load

Balancer.

Which steps should be taken to accomplish the task using the AWS Management Console?

- A. 1. Update the application code in the existing deployment. 2. Select a new load balancer type before running the deployment. 3. Deploy the new version of the application code to the environment.
- B. 1. Create a new environment with the same configurations except for the load balancer type. 2. Deploy the same application version as used in the original environment. 3. Run the swap-environment-cnames action.
- C. 1. Clone the existing environment, changing the associated load balancer type. 2. Deploy the same application version as used in the original environment. 3. Run the swap-environment-cnames action.
- D. 1. Edit the environment definitions in the existing deployment. 2. Change the associated load balancer type according to the requirements. 3. Rebuild the environment with the new load balancer type.

Answer: B

Question #201

A Developer must encrypt a 100-GB object using AWS KMS.

What is the BEST approach?

- A. Make an Encrypt API call to encrypt the plaintext data as ciphertext using a customer master key (CMK)
- B. Make an Encrypt API call to encrypt the plaintext data as ciphertext using a customer master key (CMK) with imported key material
- C. Make an GenerateDataKey API call that returns a plaintext key and an encrypted copy of a data key. Use a plaintext key to encrypt the data
- D. Make an GenerateDataKeyWithoutPlaintext API call that returns an encrypted copy of a data key. Use an encrypted key to encrypt the data

Answer: C

Question #202

<https://itexamcertified.com>

<https://itexamcertified.com>

A Development team would like to migrate their existing application code from a GitHub repository to AWS CodeCommit.

What needs to be created before they can migrate a cloned repository to CodeCommit over HTTPS?

- A. A GitHub secure authentication token
- B. A public and private SSH key file
- C. A set of Git credentials generated from IAM
- D. An Amazon EC2 IAM role with CodeCommit permissions

Answer: C

Reference:

<https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-migrate-repository-existing.html>

Question #203

A Developer is writing a REST service that will add items to a shopping list. The service is built on Amazon API Gateway with AWS Lambda integrations. The shopping list items are send as query string parameters in the method request.

How should the Developer convert the query string parameters to arguments for the Lambda function?

- A. Enable request validation
- B. Include the Amazon Resource Name (ARN) of the Lambda function
- C. Change the integration type
- D. Create a mapping template C

Answer: D

Reference:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-create-api-step-by-step.html>

Question #204

When developing an AWS Lambda function that processes Amazon Kinesis Data Streams, Administrators within the company must receive a notice that includes the processed data.

How should the Developer write the function to send processed data to the Administrators?

- A. Separate the Lambda handler from the core logic
- B. Use Amazon CloudWatch Events to send the processed data

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. Publish the processed data to an Amazon SNS topic
- D. Push the processed data to Amazon SQS

Answer: C

Question #205

A Developer is storing documents in Amazon S3 that will require encryption at rest. The encryption keys must be rotated annually, at least.

What is the easiest way to achieve this?

- A. Encrypt the data before sending it to Amazon S3
- B. Import a custom key into AWS KMS with annual rotation enabled
- C. Use AWS KMS with automatic key rotation
- D. Export a key from AWS KMS to encrypt the data

Answer: C

Question #206

A company is creating a REST service using an Amazon API Gateway with AWS Lambda integration. The service runs different versions for testing purposes.

What would be the BEST way to accomplish this?

- A. Use an x-Version header to denote which version is being called and pass that header to the Lambda function(s)
- B. Create an API Gateway Lambda authorizer to route API clients to the correct API version
- C. Create an API Gateway resource policy to isolate versions and provide context to the Lambda function(s)
- D. Deploy the API versions as unique stages with unique endpoints and use stage variables to provide further context

Answer: D

Question #207

A company wants to implement authentication for its new REST service using Amazon API Gateway. To authenticate the calls, each request must include HTTP headers with a client ID and user ID. These credentials must be compared to authentication data in an Amazon DynamoDB table.

<https://itexamcertified.com>

What MUST the company do to implement this authentication in API Gateway?

- A. Implement an AWS Lambda authorizer that references the DynamoDB authentication table
- B. Create a model that requires the credentials, then grant API Gateway access to the authentication table
- C. Modify the integration requests to require the credentials, then grant API Gateway access to the authentication table
- D. Implement an Amazon Cognito authorizer that references the DynamoDB authentication table

Answer: D

Question #208

An Amazon RDS database instance is used by many applications to look up historical data. The query rate is relatively constant. When the historical data is updated each day, the resulting write traffic slows the read query performance and affects all application users.

What can be done to eliminate the performance impact on application users?

- A. Make sure Amazon RDS is Multi-AZ so it can better absorb increased traffic.
- B. Create an RDS Read Replica and direct all read traffic to the replica.
- C. Implement Amazon ElastiCache in front of Amazon RDS to buffer the write traffic.
- D. Use Amazon DynamoDB instead of Amazon RDS to buffer the read traffic. B

Answer:B

Set 2

Question #1

Company C is currently hosting their corporate site in an Amazon S3 bucket with Static Website Hosting enabled. Currently, when visitors go to <http://www.companyc.com> the index.html page is returned. Company C now would like a new page welcome.html to be returned when a visitor enters <http://www.companyc.com> in the browser.

Which of the following steps will allow Company C to meet this requirement? (Choose two.)

- A. Upload an html page named welcome.html to their S3 bucket
- B. Create a welcome subfolder in their S3 bucket
- C. Set the Index Document property to welcome.html
- D. Move the index.html page to a welcome subfolder
- E. Set the Error Document property to welcome.html

<https://itexamcertified.com>

Answer: AC

Question #2

What type of block cipher does Amazon S3 offer for server side encryption?

- A. Triple DES
- B. Advanced Encryption Standard
- C. Blowfish
- D. RC5

Answer: B

Question #3

If an application is storing hourly log files from thousands of instances from a high traffic web site, which naming scheme would give optimal performance on S3?

- A. Sequential
- B. instanceID_log-HH-DD-MM-YYYY
- C. instanceID_log-YYYY-MM-DD-HH
- D. HH-DD-MM-YYYY-log_instanceID
- E. YYYY-MM-DD-HH-log_instanceID

Answer: D

Question #4

Which of the following statements about SQS is true?

- A. Messages will be delivered exactly once and messages will be delivered in First in, First out order
- B. Messages will be delivered exactly once and message delivery order is indeterminate
- C. Messages will be delivered one or more times and messages will be delivered in First in, First out order
- D. Messages will be delivered one or more times and message delivery order is indeterminate

Answer: D

<https://itexamcertified.com>

Question #5

A corporate web application is deployed within an Amazon VPC, and is connected to the corporate data center via IPsec VPN. The application must authenticate against the on-premise LDAP server. Once authenticated, logged-in users can only access an S3 keyspace specific to the user.

Which two approaches can satisfy the objectives? (Choose two.)

- A. The application authenticates against LDAP. The application then calls the IAM Security Service to login to IAM using the LDAP credentials. The application can use the IAM temporary credentials to access the appropriate S3 bucket.
- B. The application authenticates against LDAP, and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service to assume that IAM Role. The application can use the temporary credentials to access the appropriate S3 bucket.
- C. The application authenticates against IAM Security Token Service using the LDAP credentials. The application uses those temporary AWS security credentials to access the appropriate S3 bucket.
- D. Develop an identity broker which authenticates against LDAP, and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.
- E. Develop an identity broker which authenticates against IAM Security Token Service to assume an IAM Role to get temporary AWS security credentials. The application calls the identity broker to get AWS

Answer: BD

Question #6

Company B provides an online image recognition service and utilizes SQS to decouple system components for scalability. The SQS consumers poll the imaging queue as often as possible to keep end-to-end throughput as high as possible. However, Company B is realizing that polling in tight loops is burning CPU cycles and increasing costs with empty responses.

How can Company B reduce the number of empty responses?

- A. Set the imaging queue visibility Timeout attribute to 20 seconds
- B. Set the Imaging queue ReceiveMessageWaitTimeSeconds attribute to 20 seconds
- C. Set the imaging queue MessageRetentionPeriod attribute to 20 seconds
- D. Set the DelaySeconds parameter of a message to 20 seconds

Answer: B

Question #7

An Amazon S3 bucket, "myawsbucket" is configured with website hosting in Tokyo region, what is the region-specific website endpoint?

- A. www.myawsbucket.ap-northeast-1.amazonaws.com
- B. myawsbucket.s3-website-ap-northeast-1.amazonaws.com
- C. myawsbucket.amazonaws.com
- D. myawsbucket.tokyo.amazonaws.com

Answer: B

Question #8

You are inserting 1000 new items every second in a DynamoDB table. Once an hour these items are analyzed and then are no longer needed. You need to minimize provisioned throughput, storage, and API calls.

Given these requirements, what is the most efficient way to manage these items after the analysis?

- A. Retain the items in a single table
- B. Delete items individually over a 24 hour period
- C. Delete the table and create a new table per hour
- D. Create a new table per hour

Answer: C

Question #9

You have written an application that uses the Elastic Load Balancing service to spread traffic to several web servers. Your users complain that they are sometimes forced to login again in the middle of using your application, after they have already logged in. This is not behavior you have designed.

What is a possible solution to prevent this happening?

- A. Use instance memory to save session state.
- B. Use instance storage to save session state.
- C. Use EBS to save session state
- D. Use ElastiCache to save session state.
- E. Use Glacier to save session slate.

<https://itexamcertified.com>

Answer: D

Question #10

You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site. At some point you find out that other sites have been linking to the photos on your site, causing loss to your business.

What is an effective method to mitigate this?

- A. Store photos on an EBS volume of the web server
- B. Remove public read access and use signed URLs with expiry dates.
- C. Use CloudFront distributions for static content.
- D. Block the IPs of the offending websites in Security Groups.

Answer: B

Question #11

Which statements about DynamoDB are true? (Choose two.)

- A. DynamoDB uses a pessimistic locking model
- B. DynamoDB uses optimistic concurrency control
- C. DynamoDB uses conditional writes for consistency
- D. DynamoDB restricts item access during reads
- E. DynamoDB restricts item access during writes

Answer: BC

Question #12

You are providing AWS consulting services for a company developing a new mobile application that will be leveraging Amazon SNS Mobile Push for push notifications. In order to send direct notification messages to individual devices each device registration identifier or token needs to be registered with SNS; however the developers are not sure of the best way to do this.

You advise them to:

- A. Bulk upload the device tokens contained in a CSV file via the AWS Management Console.
- B. Let the push notification service (e.g. Amazon Device Messaging) handle the registration.
- C. Implement a token vending service to handle the registration.

<https://itexamcertified.com>

<https://itexamcertified.com>

D. Call the CreatePlatformEndPoint API function to register multiple device tokens.

Answer: D

Question #13

You are writing to a DynamoDB table and receive the following exception:"

ProvisionedThroughputExceeded". though according to your Cloudwatch metrics for the table, you are not exceeding your provisioned throughput.

What could be an explanation for this?

- A. You haven't provisioned enough DynamoDB storage instances
- B. You're exceeding your capacity on a particular Range Key
- C. You're exceeding your capacity on a particular Hash Key
- D. You're exceeding your capacity on a particular Sort Key
- E. You haven't configured DynamoDB Auto Scaling triggers

Answer: C

Question #14

Which of the following services are included at no additional cost with the use of the AWS platform? (Choose two.)

- A. Simple Storage Service
- B. Elastic Compute Cloud
- C. Auto Scaling
- D. Elastic Load Balancing
- E. CloudFormation
- F. Simple Workflow Service

Answer: CE

Question #15

Your application is trying to upload a 6 GB file to Simple Storage Service and receive a "Your proposed upload exceeds the maximum allowed object size." error message.

<https://itexamcertified.com>

<https://itexamcertified.com>

What is a possible solution for this?

- A. None, Simple Storage Service objects are limited to 5 GB
- B. Use the multi-part upload API for this object
- C. Use the large object upload API for this object
- D. Contact support to increase your object size limit
- E. Upload to a different region

Answer: B

Question #16

What AWS products and features can be deployed by Elastic Beanstalk? (Choose three.)

- A. Auto scaling groups
- B. Route 53 hosted zones
- C. Elastic Load Balancers
- D. RDS Instances
- E. Elastic IP addresses
- F. SQS Queues

Answer: ACD

Question #17

Games-R-Us is launching a new game app for mobile devices. Users will log into the game using their existing Facebook account and the game will record player data and scoring information directly to a DynamoDB table. What is the most secure approach for signing requests to the DynamoDB API?

- A. Create an IAM user with access credentials that are distributed with the mobile app to sign the requests
- B. Distribute the AWS root account access credentials with the mobile app to sign the requests
- C. Request temporary security credentials using web identity federation to sign the requests
- D. Establish cross account access between the mobile app and the DynamoDB table to sign the requests

Answer: C

<https://itexamcertified.com>

Question #18

Which of the following programming languages have an officially supported AWS SDK? (Choose two.)

A. Perl

B. PHP

C. Pascal

D. Java

E. SQL

Answer: BD

Question #19

A meteorological system monitors 600 temperature gauges, obtaining temperature samples every minute and saving each sample to a DynamoDB table. Each sample involves writing 1K of data and the writes are evenly distributed over time.

How much write throughput is required for the target table?

A. 1 write capacity unit

B. 10 write capacity units

C. 60 write capacity units

D. 600 write capacity units

E. 3600 write capacity units

Answer: B

Question #20

In DynamoDB, what type of HTTP response codes indicate that a problem was found with the client request sent to the service?

A. 5xx HTTP response code

B. 200 HTTP response code

C. 306 HTTP response code

D. 4xx HTTP response code

Answer: D

Question #21

Company C has recently launched an online commerce site for bicycles on AWS. They have a "Product" DynamoDB table that stores details for each bicycle, such as, manufacturer, color, price, quantity and size to display in the online store. Due to customer demand, they want to include an image for each bicycle along with the existing details.

Which approach below provides the least impact to provisioned throughput on the "Product" table?

- A. Serialize the image and store it in multiple DynamoDB tables
- B. Create an "Images" DynamoDB table to store the Image with a foreign key constraint to the "Product" table
- C. Add an image data type to the "Product" table to store the images in binary format
- D. Store the images in Amazon S3 and add an S3 URL pointer to the "Product" table item for each image

Answer: D

Question #22

Which DynamoDB limits can be raised by contacting AWS support? (Choose two.)

- A. The number of hash keys per account
- B. The maximum storage used per account
- C. The number of tables per account
- D. The number of local secondary indexes per account
- E. The number of provisioned throughput units per account

Answer: CE

Question #23

When a Simple Queue Service message triggers a task that takes 5 minutes to complete, which process below will result in successful processing of the message and remove it from the queue while minimizing the chances of duplicate processing?

- A. Retrieve the message with an increased visibility timeout, process the message, delete the message from the queue
- B. Retrieve the message with an increased visibility timeout, delete the message from the queue, process the message
- C. Retrieve the message with increased DelaySeconds, process the message, delete the message from the queue

<https://itexamcertified.com>

D. Retrieve the message with increased DelaySeconds, delete the message from the queue, process the

Answer: A

Question #24

Company A has an S3 bucket containing premier content that they intend to make available to only paid subscribers of their website. The S3 bucket currently has default permissions of all objects being private to prevent inadvertent exposure of the premier content to non-paying website visitors.

How can Company A provide only paid subscribers the ability to download a premier content file in the S3 bucket?

- A. Apply a bucket policy that grants anonymous users to download the content from the S3 bucket
- B. Generate a pre-signed object URL for the premier content file when a paid subscriber requests a download
- C. Add a bucket policy that requires Multi-Factor Authentication for requests to access the S3 bucket objects
- D. Enable server side encryption on the S3 bucket for data protection against the non-paying website visitors

Answer: B

Question #25

Which of the following is an example of a good DynamoDB hash key schema for provisioned throughput efficiency?

- A. User ID, where the application has many different users.
- B. Status Code where most status codes are the same
- C. Device ID, where one is by far more popular than all the others.
- D. Game Type, where there are three possible game types

Answer: A

Question #26

An application stores payroll information nightly in DynamoDB for a large number of employees across hundreds of offices. Item attributes consist of individual name, office identifier, and cumulative daily hours.

Managers run reports for ranges of names working in their office. One query is. "Return all Items in this office for names starting with A through E".

Which table configuration will result in the lowest impact on provisioned throughput for this query?

- A. Configure the table to have a hash index on the name attribute, and a range index on the office identifier

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Configure the table to have a range index on the name attribute, and a hash index on the office identifier
- C. Configure a hash index on the name attribute and no range index
- D. Configure a hash index on the office Identifier attribute and no range index

Answer: B

Question #27

What is one key difference between an Amazon EBS-backed and an instance-store backed instance?

- A. Virtual Private Cloud requires EBS backed instances
- B. Amazon EBS-backed instances can be stopped and restarted
- C. Auto scaling requires using Amazon EBS-backed instances.
- D. Instance-store backed instances can be stopped and restarted.

Answer: B

Question #28

How can you secure data at rest on an EBS volume?

- A. Attach the volume to an instance using EC2's SSL interface.
- B. Write the data randomly instead of sequentially.
- C. Use an encrypted file system on top of the BBS volume.
- D. Encrypt the volume using the S3 server-side encryption service.
- E. Create an IAM policy that restricts read and write access to the volume.

Answer: C

Question #29

Which of the following is chosen as the default region when making an API call with an AWS SDK?

- A. ap-northeast-1
- B. us-west-2
- C. us-east-1
- D. eu-west-1

<https://itexamcertified.com>

<https://itexamcertified.com>

E. us-central-1

Answer: C

Question #30

Which of the following statements about SWF are true? (Choose three.)

- A. SWF tasks are assigned once and never duplicated
- B. SWF requires an S3 bucket for workflow storage
- C. SWF workflow executions can last up to a year
- D. SWF triggers SNS notifications on task assignment
- E. SWF uses deciders and workers to complete tasks
- F. SWF requires at least 1 EC2 instance per domain

Answer: ACE

Question #31

Which of the following are valid SNS delivery transports? (Choose two.)

- A. HTTP
- B. UDP
- C. SMS
- D. DynamoDB
- E. Named Pipes

Answer: AC

Question #32

How is provisioned throughput affected by the chosen consistency model when reading data from a DynamoDB table?

- A. Strongly consistent reads use the same amount of throughput as eventually consistent reads
- B. Strongly consistent reads use more throughput than eventually consistent reads.
- C. Strongly consistent reads use less throughput than eventually consistent reads

<https://itexamcertified.com>

<https://itexamcertified.com>

- D. Strongly consistent reads use variable throughput depending on read activity

Answer: B

Question #33

Which of the following are valid arguments for an SNS Publish request? (Choose three.)

- A. TopicArn
- B. Subject
- C. Destination
- D. Format
- E. Message
- F. Language

Answer:ABC

Question #34

How can software determine the public and private IP addresses of the Amazon EC2 instance that it is running on?

- A. Query the appropriate Amazon CloudWatch metric.
- B. Use ipconfig or ifconfig command.
- C. Query the local instance userdata.
- D. Query the local instance metadata.

Answer: D

Question #35

EC2 instances are launched from Amazon Machine Images (AMIs). A given public AMI can:

- A. be used to launch EC2 Instances in any AWS region.
- B. only be used to launch EC2 instances in the same country as the AMI is stored.
- C. only be used to launch EC2 instances in the same AWS region as the AMI is stored.
- D. only be used to launch EC2 instances in the same AWS availability zone as the AMI is stored

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: C

Question #36

Which EC2 API call would you use to retrieve a list of Amazon Machine Images (AMIs)?

- A. DescnbeInstances
- B. DescribeAMIs
- C. DescribelImages
- D. GetAMIs
- E. You cannot retrieve a list of AMIs as there are over 10,000 AMIs

Answer: C

Question #37

In AWS, which security aspects are the customer's responsibility? (Choose four.)

- A. Life-cycle management of IAM credentials
- B. Decommissioning storage devices
- C. Security Group and ACL (Access Control List) settings
- D. Encryption of EBS (Elastic Block Storage) volumes
- E. Controlling physical access to compute resources
- F. Patch management on the EC2 instance's operating system

Answer: ACDF

Question #38

When using a large Scan operation in DynamoDB, what technique can be used to minimize the impact of a scan on a table's provisioned throughput?

- A. Set a smaller page size for the scan
- B. Use parallel scans
- C. Define a range index on the table
- D. Prewarm the table by updating all items

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: C

Question #39

Company D is running their corporate website on Amazon S3 accessed from <http://www.companyd.com>. Their marketing team has published new web fonts to a separate S3 bucket accessed by the S3 endpoint <https://s3-us-west-1.amazonaws.com/cdfonts>. While testing the new web fonts, Company D recognized the web fonts are being blocked by the browser.

What should Company D do to prevent the web fonts from being blocked by the browser?

- A. Enable versioning on the cdfonts bucket for each web font
- B. Create a policy on the cdfonts bucket to enable access to everyone
- C. Add the Content-MD5 header to the request for webfonts in the cdfonts bucket from the website
- D. Configure the cdfonts bucket to allow cross-origin requests by creating a CORS configuration

Answer: D

Question #40

Which of the following platforms are supported by Elastic Beanstalk? (Choose two.)

- A. Apache Tomcat
- B. .NET
- C. IBM Websphere
- D. Oracle JBoss
- E. Jetty

Answer: AB

Question #41

Which code snippet below returns the URL of a load balanced web site created in CloudFormation with an AWS::ElasticLoadBalancing::LoadBalancer resource name "ElasticLoad Balancer"?

- A. "Fn::Join" : [".", ["http://", {"Fn::GetAttr" : ["ElasticLoadBalancer", "DNSName"]}]]
- B. "Fn::Join" : [".", ["http://", {"Fn::GetAttr" : ["ElasticLoadBalancer", "Url"]}]]
- C. "Fn::Join" : [".", ["http://", {"Ref" : "ElasticLoadBalancerUrl"}]]
- D. "Fn::Join" : [".", ["http://", {"Ref" : "ElasticLoadBalancerDNSName"}]]

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: BD

Question #42

Which features can be used to restrict access to data in S3? (Choose two.)

- A. Use S3 Virtual Hosting
- B. Set an S3 Bucket policy.
- C. Enable IAM Identity Federation.
- D. Set an S3 ACL on the bucket or the object.
- E. Create a CloudFront distribution for the bucket

Answer: BD

Question #43

What happens, by default, when one of the resources in a CloudFormation stack cannot be created?

- A. Previously-created resources are kept but the stack creation terminates.
- B. Previously-created resources are deleted and the stack creation terminates.
- C. The stack creation continues, and the final results indicate which steps failed.
- D. CloudFormation templates are parsed in advance so stack creation is guaranteed to succeed.

Answer: B

Question #44

Which of the following are correct statements with policy evaluation logic in AWS Identity and Access Management? (Choose two.)

- A. By default, all requests are denied
- B. An explicit allow overrides an explicit deny
- C. An explicit allow overrides default deny.
- D. An explicit deny does not override an explicit allow
- E. By default, all requests are allowed

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: AC

Question #45

You have an environment that consists of a public subnet using Amazon VPC and 3 instances that are running in this subnet. These three instances can successfully communicate with other hosts on the Internet. You launch a fourth instance in the same subnet, using the same AMI and security group configuration you used for the others, but find that this instance cannot be accessed from the Internet.

What should you do to enable internet access?

- A. Deploy a NAT instance into the public subnet.
- B. Modify the routing table for the public subnet
- C. Configure a publically routable IP Address In the host OS of the fourth instance.
- D. Assign an Elastic IP address to the fourth instance.

Answer: D

Question #46

If a message is retrieved from a queue in Amazon SQS, how long is the message inaccessible to other users by default?

- A. 0 seconds
- B. 1 hour
- C. 1 day
- D. forever
- E. 30 seconds

Answer: E

Question #47

What is the format of structured notification messages sent by Amazon SNS?

- A. An XML object containing MessageId, UnsubscribeURL, Subject, Message and other values
- B. An JSON object containing MessageId, DuplicateFlag, Message and other values
- C. An XML object containing MessageId, DuplicateFlag, Message and other values
- D. An JSON object containing MessageId, unsubscribeURL, Subject, Message and other values

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: D

Question #48

Which of the following services are key/value stores? (Choose three.)

- A. Amazon ElastiCache
- B. Simple Notification Service
- C. DynamoDB
- D. Simple Workflow Service
- E. Simple Storage Service

Answer: ACE

Question #49

When uploading an object, what request header can be explicitly specified in a request to Amazon S3 to encrypt object data when saved on the server side?

- A. x-amz-storage-class
- B. Content-MD5
- C. x-amz-security-token
- D. x-amz-server-side-encryption

Answer: D

Question #50

What item operation allows the retrieval of multiple items from a DynamoDB table in a single API call?

- A. GetItem
- B. BatchGetItem
- C. GetMultipleItems
- D. GetItemRange

Answer: B

<https://itexamcertified.com>

Question #51

After launching an instance that you intend to serve as a NAT (Network Address Translation) device in a public subnet you modify your route tables to have the NAT device be the target of internet bound traffic of your private subnet. When you try and make an outbound connection to the Internet from an instance in the private subnet, you are not successful.

Which of the following steps could resolve the issue?

- A. Attaching a second Elastic Network interface (ENI) to the NAT instance, and placing it in the private subnet
- B. Attaching a second Elastic Network Interface (ENI) to the instance in the private subnet, and placing it in the public subnet
- C. Disabling the Source/Destination Check attribute on the NAT instance
- D. Attaching an Elastic IP address to the instance in the private subnet

Answer: C

Question #52

You attempt to store an object in the US-STANDARD region in Amazon S3, and receive a confirmation that it has been successfully stored. You then immediately make another API call and attempt to read this object. S3 tells you that the object does not exist.

What could explain this behavior?

- A. US-STANDARD uses eventual consistency and it can take time for an object to be readable in a bucket
- B. Objects in Amazon S3 do not become visible until they are replicated to a second region.
- C. US-STANDARD imposes a 1 second delay before new objects are readable.
- D. You exceeded the bucket object limit, and once this limit is raised the object will be visible.

Answer: A

Question #53

What is the maximum number of S3 Buckets available per AWS account?

- A. 100 per region
- B. there is no limit
- C. 100 per account
- D. 500 per account

<https://itexamcertified.com>

- E. 100 per IAM user

Answer: C

Question #54

Which of the following items are required to allow an application deployed on an EC2 instance to write data to a DynamoDB table?

Assume that no security Keys are allowed to be stored on the EC2 instance. (Choose two.)

- A. Create an IAM User that allows write access to the DynamoDB table.
- B. Add an IAM Role to a running EC2 instance.
- C. Add an IAM User to a running EC2 Instance.
- D. Launch an EC2 Instance with the IAM Role included in the launch configuration.
- E. Create an IAM Role that allows write access to the DynamoDB table.
- F. Launch an EC2 Instance with the IAM User included in the launch configuration.

Answer: DE

Question #55

Company C is currently hosting their corporate site in an Amazon S3 bucket with Static Website Hosting enabled. Currently, when visitors go to <http://www.companyc.com> the index.html page is returned. Company C now would like a new page welcome.html to be returned when a visitor enters <http://www.companyc.com> in the browser.

Which of the following steps will allow Company C to meet this requirement? (Choose two.)

- A. Upload an html page named welcome.html to their S3 bucket
- B. Create a welcome subfolder in their S3 bucket
- C. Set the Index Document property to welcome.html
- D. Move the index.html page to a welcome subfolder
- E. Set the Error Document property to welcome.html

Answer: AC

Question #56

What type of block cipher does Amazon S3 offer for server side encryption?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Triple DES
- B. Advanced Encryption Standard
- C. Blowfish
- D. RC5

Answer: B

Question #57

If an application is storing hourly log files from thousands of instances from a high traffic web site, which naming scheme would give optimal performance on S3?

- A. Sequential
- B. instanceID_log-HH-DD-MM-YYYY
- C. instanceID_log-YYYY-MM-DD-HH
- D. HH-DD-MM-YYYY-log_instanceID
- E. YYYY-MM-DD-HH-log_instanceID

Answer: D

Question #58

Which of the following statements about SQS is true?

- A. Messages will be delivered exactly once and messages will be delivered in First in, First out order
- B. Messages will be delivered exactly once and message delivery order is indeterminate
- C. Messages will be delivered one or more times and messages will be delivered in First in, First out order
- D. Messages will be delivered one or more times and message delivery order is indeterminate

Answer: D

Question #59

A corporate web application is deployed within an Amazon VPC, and is connected to the corporate data center via IPsec VPN. The application must authenticate against the on-premise LDAP server. Once authenticated, logged-in users can only access an S3 keyspace specific to the user.

Which two approaches can satisfy the objectives? (Choose two.)

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. The application authenticates against LDAP. The application then calls the IAM Security Service to login to IAM using the LDAP credentials. The application can use the IAM temporary credentials to access the appropriate S3 bucket.
- B. The application authenticates against LDAP, and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service to assume that IAM Role. The application can use the temporary credentials to access the appropriate S3 bucket.
- C. The application authenticates against IAM Security Token Service using the LDAP credentials. The application uses those temporary AWS security credentials to access the appropriate S3 bucket.
- D. Develop an identity broker which authenticates against LDAP, and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.
- E. Develop an identity broker which authenticates against IAM Security Token Service to assume an IAM Role to get temporary AWS security credentials. The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.

Answer: BD

Question #60

Company B provides an online image recognition service and utilizes SQS to decouple system components for scalability. The SQS consumers poll the imaging queue as often as possible to keep end-to-end throughput as high as possible. However, Company B is realizing that polling in tight loops is burning CPU cycles and increasing costs with empty responses.

How can Company B reduce the number of empty responses?

- A. Set the imaging queue visibility Timeout attribute to 20 seconds
- B. Set the Imaging queue ReceiveMessageWaitTimeSeconds attribute to 20 seconds
- C. Set the imaging queue MessageRetentionPeriod attribute to 20 seconds
- D. Set the DelaySeconds parameter of a message to 20 seconds

Answer: B

Question #61

An Amazon S3 bucket, "myawsbucket" is configured with website hosting in Tokyo region, what is the region-specific website endpoint?

- A. www.myawsbucket.ap-northeast-1.amazonaws.com
- B. myawsbucket.s3-website-ap-northeast-1.amazonaws.com

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. myawsbucket.amazonaws.com
- D. myawsbucket.tokyo.amazonaws.com

Answer: B

Question #62

You are inserting 1000 new items every second in a DynamoDB table. Once an hour these items are analyzed and then are no longer needed. You need to minimize provisioned throughput, storage, and API calls.

Given these requirements, what is the most efficient way to manage these items after the analysis?

- A. Retain the items in a single table
- B. Delete items individually over a 24 hour period
- C. Delete the table and create a new table per hour
- D. Create a new table per hour

Answer: C

on #63

You have written an application that uses the Elastic Load Balancing service to spread traffic to several web servers. Your users complain that they are sometimes forced to log in again in the middle of using your application, after they have already logged in. This is not behavior you have designed.

What is a possible solution to prevent this happening?

- A. Use instance memory to save session state.
- B. Use instance storage to save session state.
- C. Use EBS to save session state
- D. Use ElastiCache to save session state.
- E. Use Glacier to save session slate.

Answer: D

Question #64

You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site. At some point you find out that other sites have been linking to the photos on your site, causing loss to your business.

<https://itexamcertified.com>

<https://itexamcertified.com>

What is an effective method to mitigate this?

- A. Store photos on an EBS volume of the web server
- B. Remove public read access and use signed URLs with expiry dates.
- C. Use CloudFront distributions for static content.
- D. Block the IPs of the offending websites in Security Groups.

Answer: B

Question #65

Which statements about DynamoDB are true? (Choose two.)

- A. DynamoDB uses a pessimistic locking model
- B. DynamoDB uses optimistic concurrency control
- C. DynamoDB uses conditional writes for consistency
- D. DynamoDB restricts item access during reads
- E. DynamoDB restricts item access during writes

Answer: BC

Question #66

You are providing AWS consulting services for a company developing a new mobile application that will be leveraging Amazon SNS Mobile Push for push notifications. In order to send direct notification messages to individual devices each device registration identifier or token needs to be registered with SNS; however the developers are not sure of the best way to do this.

You advise them to:

- A. Bulk upload the device tokens contained in a CSV file via the AWS Management Console.
- B. Let the push notification service (e.g. Amazon Device Messaging) handle the registration.
- C. Implement a token vending service to handle the registration.
- D. Call the CreatePlatformEndPoint API function to register multiple device tokens.

Answer: D

Question #67

<https://itexamcertified.com>

<https://itexamcertified.com>

You are writing to a DynamoDB table and receive the following exception: "ProvisionedThroughputExceededException". though according to your Cloudwatch metrics for the table, you are not exceeding your provisioned throughput.

What could be an explanation for this?

- A. You haven't provisioned enough DynamoDB storage instances
- B. You're exceeding your capacity on a particular Range Key
- C. You're exceeding your capacity on a particular Hash Key
- D. You're exceeding your capacity on a particular Sort Key
- E. You haven't configured DynamoDB Auto Scaling triggers

Answer: C

Question #68

Which of the following services are included at no additional cost with the use of the AWS platform? (Choose two.)

- A. Simple Storage Service
- B. Elastic Compute Cloud
- C. Auto Scaling
- D. Elastic Load Balancing
- E. CloudFormation
- F. Simple Workflow Service

Answer: CE

Question #69

Your application is trying to upload a 6 GB file to Simple Storage Service and receive a "Your proposed upload exceeds the maximum allowed object size." error message.

What is a possible solution for this?

- A. None, Simple Storage Service objects are limited to 5 GB
- B. Use the multi-part upload API for this object
- C. Use the large object upload API for this object
- D. Contact support to increase your object size limit
- E. Upload to a different region

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: B

Question #70

What AWS products and features can be deployed by Elastic Beanstalk? (Choose three.)

- A. Auto scaling groups
- B. Route 53 hosted zones
- C. Elastic Load Balancers
- D. RDS Instances
- E. Elastic IP addresses
- F. SQS Queues

Answer: ACD

Question #71

Games-R-Us is launching a new game app for mobile devices. Users will log into the game using their existing Facebook account and the game will record player data and scoring information directly to a DynamoDB table.

What is the most secure approach for signing requests to the DynamoDB API?

- A. Create an IAM user with access credentials that are distributed with the mobile app to sign the requests
- B. Distribute the AWS root account access credentials with the mobile app to sign the requests
- C. Request temporary security credentials using web identity federation to sign the requests
- D. Establish cross account access between the mobile app and the DynamoDB table to sign the requests

Answer: C

Question #72

Which of the following programming languages have an officially supported AWS SDK? (Choose two.)

- A. Perl
- B. PHP
- C. Pascal
- D. Java

<https://itexamcertified.com>

E. SQL

Answer: BD

Question #73

A meteorological system monitors 600 temperature gauges, obtaining temperature samples every minute and saving each sample to a DynamoDB table. Each sample involves writing 1K of data and the writes are evenly distributed over time.

How much write throughput is required for the target table?

- A. 1 write capacity unit
- B. 10 write capacity units
- C. 60 write capacity units
- D. 600 write capacity units
- E. 3600 write capacity units

Answer: B

Question #74

In DynamoDB, what type of HTTP response codes indicate that a problem was found with the client request sent to the service?

- A. 5xx HTTP response code
- B. 200 HTTP response code
- C. 306 HTTP response code
- D. 4xx HTTP response code

Question #75

Company C has recently launched an online commerce site for bicycles on AWS. They have a "Product" DynamoDB table that stores details for each bicycle, such as, manufacturer, color, price, quantity and size to display in the online store. Due to customer demand, they want to include an image for each bicycle along with the existing details.

Which approach below provides the least impact to provisioned throughput on the "Product" table?

- A. Serialize the image and store it in multiple DynamoDB tables
- B. Create an "Images" DynamoDB table to store the Image with a foreign key constraint to the "Product" table

<https://itexamcertified.com>

- C. Add an image data type to the "Product" table to store the images in binary format
- D. Store the images in Amazon S3 and add an S3 URL pointer to the "Product" table item for each image

Answer: D

Question #76

Which DynamoDB limits can be raised by contacting AWS support? (Choose two.)

- A. The number of hash keys per account
- B. The maximum storage used per account
- C. The number of tables per account
- D. The number of local secondary indexes per account
- E. The number of provisioned throughput units per account

Answer: CE

Question #77

When a Simple Queue Service message triggers a task that takes 5 minutes to complete, which process below will result in successful processing of the message and remove it from the queue while minimizing the chances of duplicate processing?

- A. Retrieve the message with an increased visibility timeout, process the message, delete the message from the queue
- B. Retrieve the message with an increased visibility timeout, delete the message from the queue, process the message
- C. Retrieve the message with increased DelaySeconds, process the message, delete the message from the queue
- D. Retrieve the message with increased DelaySeconds, delete the message from the queue, process the message

Answer: A

Question #78

Company A has an S3 bucket containing premier content that they intend to make available to only paid subscribers of their website. The S3 bucket currently has default permissions of all objects being private to prevent inadvertent exposure of the premier content to non-paying website visitors.

How can Company A provide only paid subscribers the ability to download a premier content file in the S3 bucket?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Apply a bucket policy that grants anonymous users to download the content from the S3 bucket
- B. Generate a pre-signed object URL for the premier content file when a paid subscriber requests a download
- C. Add a bucket policy that requires Multi-Factor Authentication for requests to access the S3 bucket objects
- D. Enable server side encryption on the S3 bucket for data protection against the non-paying website visitors

Answer: B

Question #79

Which of the following is an example of a good DynamoDB hash key schema for provisioned throughput efficiency?

- A. User ID, where the application has many different users.
- B. Status Code where most status codes are the same
- C. Device ID, where one is by far more popular than all the others.
- D. Game Type, where there are three possible game types

Answer: A

Question #80

An application stores payroll information nightly in DynamoDB for a large number of employees across hundreds of offices. Item attributes consist of individual name, office identifier, and cumulative daily hours. Managers run reports for ranges of names working in their office. One query is. "Return all Items in this office for names starting with A through E".

Which table configuration will result in the lowest impact on provisioned throughput for this query?

- A. Configure the table to have a hash index on the name attribute, and a range index on the office identifier
- B. Configure the table to have a range index on the name attribute, and a hash index on the office identifier
- C. Configure a hash index on the name attribute and no range index
- D. Configure a hash index on the office Identifier attribute and no range index

Answer: B

Question #81

What is one key difference between an Amazon EBS-backed and an instance-store backed instance?

- A. Virtual Private Cloud requires EBS backed instances

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Amazon EBS-backed instances can be stopped and restarted
- C. Auto scaling requires using Amazon EBS-backed instances.
- D. Instance-store backed instances can be stopped and restarted.

Answer: B

Question #82

How can you secure data at rest on an EBS volume?

- A. Attach the volume to an instance using EC2's SSL interface.
- B. Write the data randomly instead of sequentially.
- C. Use an encrypted file system on top of the BBS volume.
- D. Encrypt the volume using the S3 server-side encryption service.
- E. Create an IAM policy that restricts read and write access to the volume.

Answer: C

Question #83

Which of the following is chosen as the default region when making an API call with an AWS SDK?

- A. ap-northeast-1
- B. us-west-2
- C. us-east-1
- D. eu-west-1
- E. us-central-1

Answer: C

Question #84

Which of the following statements about SWF are true? (Choose three.)

- A. SWF tasks are assigned once and never duplicated
- B. SWF requires an S3 bucket for workflow storage
- C. SWF workflow executions can last up to a year

<https://itexamcertified.com>

- D. SWF triggers SNS notifications on task assignment
- E. SWF uses deciders and workers to complete tasks
- F. SWF requires at least 1 EC2 instance per domain

Answer: ACE

Question #85

Which of the following are valid SNS delivery transports? (Choose two.)

- A. HTTP
- B. UDP
- C. SMS
- D. DynamoDB
- E. Named Pipes

Answer: AC

Question #86

How is provisioned throughput affected by the chosen consistency model when reading data from a DynamoDB table?

- A. Strongly consistent reads use the same amount of throughput as eventually consistent reads
- B. Strongly consistent reads use more throughput than eventually consistent reads.
- C. Strongly consistent reads use less throughput than eventually consistent reads
- D. Strongly consistent reads use variable throughput depending on read activity

Answer: B

Question #87

Which of the following are valid arguments for an SNS Publish request? (Choose three.)

- A. TopicArn
- B. Subject
- C. Destination

<https://itexamcertified.com>

- D. Format
- E. Message
- F. Language

Answer: ABE

Question #88

How can software determine the public and private IP addresses of the Amazon EC2 instance that it is running on?

- A. Query the appropriate Amazon CloudWatch metric.
- B. Use ipconfig or ifconfig command.
- C. Query the local instance userdata.
- D. Query the local instance metadata.

Answer: D

Question #89

EC2 instances are launched from Amazon Machine images (AMIs). A given public AMI can:

- A. be used to launch EC2 Instances in any AWS region.
- B. only be used to launch EC2 instances in the same country as the AMI is stored.
- C. only be used to launch EC2 instances in the same AWS region as the AMI is stored.
- D. only be used to launch EC2 instances in the same AWS availability zone as the AMI is stored

Answer: C

Question #90

Which EC2 API call would you use to retrieve a list of Amazon Machine Images (AMIs)?

- A. DescnbeInstances
 - B. DescribeAMIs
 - C. DescribeImages
 - D. GetAMIs
- E. You cannot retrieve a list of AMIs as there are over 10,000 AMIs

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: C

Question #91

In AWS, which security aspects are the customer's responsibility? (Choose four.)

- A. Life-cycle management of IAM credentials
- B. Decommissioning storage devices
- C. Security Group and ACL (Access Control List) settings
- D. Encryption of EBS (Elastic Block Storage) volumes
- E. Controlling physical access to compute resources
- F. Patch management on the EC2 instance's operating system

Answer: ABCF

Question #92

When using a large Scan operation in DynamoDB, what technique can be used to minimize the impact of a scan on a table's provisioned throughput?

- A. Set a smaller page size for the scan
- B. Use parallel scans
- C. Define a range index on the table
- D. Prewarm the table by updating all items

Answer: A

Question #93

Company D is running their corporate website on Amazon S3 accessed from <http://www.companyd.com>. Their marketing team has published new web fonts to a separate S3 bucket accessed by the S3 endpoint <https://s3-us-west-1.amazonaws.com/cdfonts>. While testing the new web fonts, Company D recognized the web fonts are being blocked by the browser.

What should Company D do to prevent the web fonts from being blocked by the browser?

- A. Enable versioning on the cdfonts bucket for each web font
- B. Create a policy on the cdfonts bucket to enable access to everyone
- C. Add the Content-MD5 header to the request for webfonts in the cdfonts bucket from the website

<https://itexamcertified.com>

<https://itexamcertified.com>

D. Configure the cdfonts bucket to allow cross-origin requests by creating a CORS configuration

Answer: D

Question #94

Which of the following platforms are supported by Elastic Beanstalk? (Choose two.)

- A. Apache Tomcat
- B. .NET
- C. IBM Websphere
- D. Oracle JBoss
- E. Jetty

Answer: AB

Question #95

Which code snippet below returns the URL of a load balanced web site created in CloudFormation with an AWS::ElasticLoadBalancing::LoadBalancer resource name "ElasticLoad Balancer"?

- A. "Fn::Join" : [".", ["http://", {"Fn::GetAttr" : ["ElasticLoadBalancer", "DNSName"]}]]
- B. "Fn::Join" : [".", ["http://", {"Fn::GetAttr" : ["ElasticLoadBalancer", "Url"]}]]
- C. "Fn::Join" : [".", ["http://", {"Ref" : "ElasticLoadBalancerUrl"}]]
- D. "Fn::Join" : [".", ["http://", {"Ref" : "ElasticLoadBalancerDNSName"}]]

Answer: A

Question #96

Which features can be used to restrict access to data in S3? (Choose two.)

- A. Use S3 Virtual Hosting
- B. Set an S3 Bucket policy.
- C. Enable IAM Identity Federation.
- D. Set an S3 ACL on the bucket or the object.
- E. Create a CloudFront distribution for the bucket

<https://itexamcertified.com>

Answer: BD

Question #97

What happens, by default, when one of the resources in a CloudFormation stack cannot be created?

- A. Previously-created resources are kept but the stack creation terminates.
- B. Previously-created resources are deleted and the stack creation terminates.
- C. The stack creation continues, and the final results indicate which steps failed.
- D. CloudFormation templates are parsed in advance so stack creation is guaranteed to succeed.

Answer: B

Question #98

Which of the following are correct statements with policy evaluation logic in AWS Identity and Access Management? (Choose two.)

- A. By default, all requests are denied
- B. An explicit allow overrides an explicit deny
- C. An explicit allow overrides default deny.
- D. An explicit deny does not override an explicit allow
- E. By default, all request are allowed

Answer: AC

Question #99

You have an environment that consists of a public subnet using Amazon VPC and 3 instances that are running in this subnet. These three instances can successfully communicate with other hosts on the Internet. You launch a fourth instance in the same subnet, using the same AMI and security group configuration you used for the others, but find that this instance cannot be accessed from the Internet.

What should you do to enable internet access?

- A. Deploy a NAT instance into the public subnet.
- B. Modify the routing table for the public subnet
- C. Configure a publically routable IP Address In the host OS of the fourth instance.

<https://itexamcertified.com>

D. Assign an Elastic IP address to the fourth instance.

Answer: D

Question #100

If a message is retrieved from a queue in Amazon SQS, how long is the message inaccessible to other users by default?

- A. 0 seconds
- B. 1 hour
- C. 1 day
- D. forever
- E. 30 seconds

Answer: E

Question #101

What is the format of structured notification messages sent by Amazon SNS?

- A. An XML object containing MessageId, UnsubscribeURL, Subject, Message and other values
- B. An JSON object containing MessageId, DuplicateFlag, Message and other values
- C. An XML object containing MessageId, DuplicateFlag, Message and other values
- D. An JSON object containing MessageId, unsubscribeURL, Subject, Message and other values

Answer: D

Question #102

Which of the following services are key/value stores? (Choose three.)

- A. Amazon ElastiCache
- B. Simple Notification Service
- C. DynamoDB
- D. Simple Workflow Service
- E. Simple Storage Service

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: ACE

Question #103

When uploading an object, what request header can be explicitly specified in a request to Amazon S3 to encrypt object data when saved on the server side?

- A. x-amz-storage-class
- B. Content-MD5
- C. x-amz-security-token
- D. x-amz-server-side-encryption

Answer: D

Question #104

What item operation allows the retrieval of multiple items from a DynamoDB table in a single API call?

- A. GetItem
- B. BatchGetItem
- C. GetMultipleItems
- D. GetItemRange

Answer: B

Question #105

After launching an instance that you intend to serve as a NAT (Network Address Translation) device in a public subnet you modify your route tables to have the

NAT device be the target of internet bound traffic of your private subnet. When you try and make an outbound connection to the Internet from an instance in the private subnet, you are not successful.

Which of the following steps could resolve the issue?

- A. Attaching a second Elastic Network interface (ENI) to the NAT instance, and placing it in the private subnet
- B. Attaching a second Elastic Network Interface (ENI) to the instance in the private subnet, and placing it in the public subnet
- C. Disabling the Source/Destination Check attribute on the NAT instance

<https://itexamcertified.com>

D. Attaching an Elastic IP address to the instance in the private subnet

Answer: C

Question #106

You attempt to store an object in the US-STANDARD region in Amazon S3, and receive a confirmation that it has been successfully stored. You then immediately make another API call and attempt to read this object. S3 tells you that the object does not exist.

What could explain this behavior?

- A. US-STANDARD uses eventual consistency and it can take time for an object to be readable in a bucket
- B. Objects in Amazon S3 do not become visible until they are replicated to a second region.
- C. US-STANDARD imposes a 1 second delay before new objects are readable.
- D. You exceeded the bucket object limit, and once this limit is raised the object will be visible.

Answer: A

Question #107

What is the maximum number of S3 Buckets available per AWS account?

- A. 100 per region
- B. there is no limit
- C. 100 per account
- D. 500 per account
- E. 100 per IAM user

Answer: C

Question #108

Which of the following items are required to allow an application deployed on an EC2 instance to write data to a DynamoDB table?

Assume that no security Keys are allowed to be stored on the EC2 instance. (Choose two.)

- A. Create an IAM User that allows write access to the DynamoDB table.
- B. Add an IAM Role to a running EC2 instance.

<https://itexamcertified.com>

- C. Add an IAM User to a running EC2 Instance.
- D. Launch an EC2 Instance with the IAM Role included in the launch configuration.
- E. Create an IAM Role that allows write access to the DynamoDB table.
- F. Launch an EC2 Instance with the IAM User included in the launch configuration.

Answer: DE

Question #109

A Developer is trying to make API calls using SDK. The IAM user credentials used by the application require multi-factor authentication for all API calls.

Which method the Developer use to access the multi-factor authentication protected API?

- A. GetFederationToken
- B. GetCallerIdentity
- C. GetSessionToken
- D. DecodeAuthorizationMessage

Answer: C

Question #110

A Developer has an e-commerce API hosted on Amazon ECS. Variable and spiking demand on the application is causing order processing to take too long. The application processes Amazon SQS queues. The ApproximateNumberOfMessagesVisible metric spikes at very high values throughout the day, which cause Amazon CloudWatch alarm breaches. Other ECS metrics for the API containers are well within limits.

What can the Developer implement to improve performance while keeping costs low?

- A. Target tracking scaling policy
- B. Docker Swarm
- C. Service scheduler
- D. Step scaling policy

Answer: D

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

<https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-amazon-sns/>

Question #111

A Developer wants to build an application that will allow new users to register and create new user accounts. The application must also allow users with social media accounts to log in using their social media credentials.

Which AWS service or feature can be used to meet these requirements?

- A. AWS IAM
- B. Amazon Cognito identity pools
- C. Amazon Cognito user pools
- D. AWS Directory Service

Answer: D

Reference:

<https://aws.amazon.com/blogs/apn/how-to-authenticate-users-into-your-apps-using-application-load-balancer-and-centrify/>

Question #112

A company is developing a web application that allows its employees to upload a profile picture to a private Amazon S3 bucket. There is no size limit for the profile pictures, which should be displayed every time an employee logs in. For security reasons, the pictures cannot be publicly accessible.

What is a viable long-term solution for this scenario?

- A. Generate a presigned URL when a picture is uploaded. Save the URL in an Amazon DynamoDB table. Return the URL to the browser when the employee logs in.
- B. Save the picture's S3 key in an Amazon DynamoDB table. Create an Amazon S3 VPC endpoint to allow the employees to download pictures once they log in.
- C. Encode a picture using base64. Save the base64 string in an Amazon DB table. Allow the browser to retrieve the string and convert it to a picture.
- D. Save the picture's S3 key in an Amazon DynamoDB table. Use a function to generate a presigned URL every time an employee logs in. Return the URL to the browser.

Answer: B

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-private-connection-no-authentication/>

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #113

A Developer is going to deploy an AWS Lambda function that requires significant CPU utilization.

Which approach will MINIMIZE the average runtime of the function?

- A. Deploy the function into multiple AWS Regions.
- B. Deploy the function into multiple Availability Zones.
- C. Deploy the function using Lambda layers.
- D. Deploy the function with its memory allocation set to the maximum amount.

Answer: C

Layers let you keep your deployment package small, which makes development easier. You can avoid errors that can occur when you install and package dependencies with your function code.

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-dg.pdf>

(86)

Question #114

A company has a legacy application that was migrated to a fleet of Amazon EC2 instances. The application stores data in a MySQL database that is currently installed on a single EC2 instance. The company has decided to migrate the database from the EC2 instance to MySQL on Amazon RDS.

What should the Developer do to update the application to support data storage in Amazon RDS?

- A. Update the database connection parameters in the application to point to the new RDS instance.
- B. Add a script to the EC2 instance that implements an AWS SDK for requesting database credentials.
- C. Create a new EC2 instance with an IAM role that allows access to the new RDS database.
- D. Create an AWS Lambda function that will route traffic, from the EC2 instance to the RDS database.

Answer: A

Question #115

A Developer is working on an AWS Lambda function that accesses Amazon DynamoDB. The Lambda function must retrieve an item and update some of its attributes, or create the item if it does not exist. The Lambda function has access to the primary key.

<https://itexamcertified.com>

<https://itexamcertified.com>

Which IAM permissions should the Developer request for the Lambda function to achieve this functionality?

- A. dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem
- B. dynamodb:UpdateItem dynamodb:GetItem dynamodb:DescribeTable
- C. dynamodb:GetRecords dynamodb:PutItem dynamodb:UpdateTable
- D. dynamodb:UpdateItem dynamodb:.GetItem dynamodb:PutItem

Answer: D

Reference:

<https://docs.aws.amazon.com/AWSJavaScriptSDK/latest/AWS/DynamoDB.html>

Question #116

A Developer is storing sensitive data generated by an application in Amazon S3. The Developer wants to encrypt the data at rest. A company policy requires an audit trail of when the master key was used and by whom.

Which encryption option will meet these requirements?

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

Answer: B

Similar to SSE-S3, but with some additional benefits along with some additional charges for using this service. provides you with an audit trail of when your key was used and by whom. Additionally, you have the option to create and manage encryption keys yourself, or use a default key that is unique to you.

Question #117

A company's website runs on an Amazon EC2 instance and uses Auto Scaling to scale the environment during peak times. Website users across the world are experiencing high latency due to static content on the EC2 instance, even during non-peak hours.

Which combination of steps will resolve the latency issue? (Choose two.)

- A. Double the Auto Scaling group's maximum number of servers.
- B. Host the application code on AWS Lambda.
- C. Scale vertically by resizing the EC2 instances.

<https://itexamcertified.com>

<https://itexamcertified.com>

- D. Create an Amazon CloudFront distribution to cache the static content.
- E. Store the application's static content in Amazon S3.

Answer: DE

Reference:

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

Question #118

A Developer is leveraging a Border Gateway Protocol (BGP)-based AWS VPN connection to connect from on-premises to Amazon EC2 instances in the

Developer's account. The Developer is able to access an EC2 instance in subnet A, but is unable to access an EC2 instance in subnet B in the same VPC.

Which logs can the Developer use to verify whether the traffic is reaching subnet B?

- A. VPN logs
- B. BGP logs
- C. VPC Flow Logs
- D. AWS CloudTrail logs

Answer: C

Question #119

A Developer has created a new AWS IAM user that has s3 putObject permission to write to a specific Amazon S3 bucket. This S3 bucket uses server-side encryption with AWS KMS managed (SSE-KMS) as the default encryption. Using the access key and secret key of the IAM user, the application received an access denied error when calling the PutObject API.

How can this issue be resolved?

- A. Update the policy of the IAM user to allow the s3 Encrypt action.
- B. Update the bucket policy of the S3 bucket to allow the IAM user to upload objects.
- C. Update the policy of the IAM user to allow the kms:GenerateDataKey action.
- D. Update the ACL of the S3 bucket to allow the IAM user to upload objects.

Answer: C

<https://itexamcertified.com>

<https://itexamcertified.com>

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-access-denied-error-kms/>

Question #120

A company has a web application that uses an Amazon Cognito user pool for authentication. The company wants to create a login page with the company logo.

What should a Developer do to meet these requirements?

- A. Create a hosted user interface in Amazon Cognito and customize it with the company logo.
- B. Create a login page with the company logo and upload it to Amazon Cognito.
- C. Create a login page in Amazon API Gateway with the logo and save the link in Amazon Cognito.
- D. Upload the logo to the Amazon Cognito app settings and point to the logo on a custom login page.

Answer: D

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/cognito-hosted-web-ui/>

Question #121

A Developer wants the ability to roll back to a previous version of an AWS Lambda function in the event of errors caused by a new deployment.

How can the Developer achieve this with MINIMAL impact on users?

- A. Change the application to use an alias that points to the current version. Deploy the new version of the code. Update the alias to use the newly deployed version. If too many errors are encountered, point the alias back to the previous version.
- B. Change the application to use an alias that points to the current version. Deploy the new version of the code. Update the alias to direct 10% of users to the newly deployed version. If too many errors are encountered, send 100% of traffic to the previous version.
- C. Do not make any changes to the application. Deploy the new version of the code. If too many errors are encountered, point the application back to the previous version using the version number in the Amazon Resource Name (ARN).
- D. Create three aliases: new, existing, and router. Point the existing alias to the current version. Have the router alias direct 100% of users to the existing alias. Update the application to use the router alias. Deploy the new version of the code. Point the new alias to this version. Update the router alias to direct 10% of users to the new alias. If too many errors are encountered, send 100% of traffic to the existing alias.

Answer: B

<https://itexamcertified.com>

Question #122

A company is developing an application that will be accessed through the Amazon API Gateway REST API. Registered users should be the only ones who can access certain resources of this API. The token being used should expire automatically and needs to be refreshed periodically.

How can a Developer meet these requirements?

- A. Create an Amazon Cognito identity pool, configure the Amazon Cognito Authorizer in API Gateway, and use the temporary credentials generated by the identity pool.
- B. Create and maintain a database record for each user with a corresponding token and use an AWS Lambda authorizer in API Gateway.
- C. Create an Amazon Cognito user pool, configure the Cognito Authorizer in API Gateway, and use the identity or access token.
- D. Create an IAM user for each API user, attach an invoke permissions policy to the API, and use an IAM authorizer in API Gateway.

Answer: C

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/cognito-custom-scopes-api-gateway/>

Question #123

A Developer is working on a serverless project based in Java. Initial testing shows a cold start takes about 8 seconds on average for AWS Lambda functions.

What should the Developer do to reduce the cold start time? (Choose two.)

- A. Add the Spring Framework to the project and enable dependency injection.
- B. Reduce the deployment package by including only needed modules from the AWS SDK for Java.
- C. Increase the memory allocation setting for the Lambda function.
- D. Increase the timeout setting for the Lambda function.
- E. Change the Lambda invocation mode from synchronous to asynchronous.

Answer: BC

Reference:

<https://github.com/awslabs/aws-serverless-java-container/wiki/Quick-start---Spring-Boot>

<https://itexamcertified.com>

Question #124

A company's ecommerce website is experiencing massive traffic spikes, which are causing performance problems in the company database. Users are reporting that accessing the website takes a long time.

A Developer wants to implement a caching layer using Amazon ElastiCache. The website is required to be responsive no matter which product a user views, and the updates to product information and prices must be strongly consistent.

Which cache writing policy will satisfy these requirements?

- A. Write to the cache directly and sync the backend at a later time
- B. Write to the backend first and wait for the cache to expire
- C. Write to the cache and the backend at the same time
- D. Write to the backend first and invalidate the cache

Answer: C

Reference:

<https://aws.amazon.com/elasticsearch/faqs/>

Question #125

An online retail company has deployed a serverless application with AWS Lambda, Amazon API Gateway, Amazon S3, and Amazon DynamoDB using AWS CloudFormation. The company rolled out a new release with major upgrades to the Lambda function and deployed the release to production. Subsequently, the application stopped working.

CloudFormation. The company rolled out a new release with major upgrades to the Lambda function and deployed the release to production. Subsequently, the application stopped working.

Which solution should bring the application back up as quickly as possible?

- A. Redeploy the application on Amazon EC2 so the Lambda function can resolve dependencies
- B. Migrate DynamoDB to Amazon RDS and redeploy the Lambda function
- C. Roll back the Lambda function to the previous version
- D. Deploy the latest Lambda function in a different Region

Answer: C

Reference:

<https://github.com/awslabs/aws-sam-cli/issues/1654>

Question #126

<https://itexamcertified.com>

<https://itexamcertified.com>

A Developer is writing an application that will run on Amazon EC2 instances in an Auto Scaling group. The Developer wants to externalize session state to support the application.

Which services will meet these needs? (Choose two.)

- A. Amazon DynamoDB
- B. Amazon Cognito
- C. Amazon ElastiCache
- D. Amazon EBS
- E. Amazon SQS

Answer: AC

Reference:

<https://forums.aws.amazon.com/thread.jspa?threadID=238457>

Question #127

A Developer has a legacy application that is hosted on-premises. Other applications hosted on AWS depend on the on-premises application for proper functioning.

In case of any application errors, the Developer wants to be able to use Amazon CloudWatch to monitor and troubleshoot all applications from one place.

How can the Developer accomplish this?

- A. Install an AWS SDK on the on-premises server to automatically send logs to CloudWatch.
- B. Download the CloudWatch agent to the on-premises server. Configure the agent to use IAM user credentials with permissions for CloudWatch.
- C. Upload log files from the on-premises server to Amazon S3 and have CloudWatch read the files.
- D. Upload log files from the on-premises server to an Amazon EC2 instance and have the instance forward the logs to CloudWatch.

Answer: B

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-premise.html>

Question #128

<https://itexamcertified.com>

<https://itexamcertified.com>

An application ingests a large number of small messages and stores them in a database. The application uses AWS Lambda. A Development team is making change to the application's processing logic. In testing, it is taking more than 15 minutes to process each message. The team is concerned the current backend may time out.

Which changes should be made to the backend system to ensure each message is processed in the MOST scalable way?

- A. Add the messages to an Amazon SQS queue. Set up and Amazon EC2 instance to poll the queue and process messages as they arrive.
- B. Add the messages to an Amazon SQS queue. Set up Amazon EC2 instances in an Auto Scaling group to poll the queue and process the messages as they arrive.
- C. Create a support ticket to increase the Lambda timeout to 60 minutes to allow for increased processing time.
- D. Change the application to directly insert the body of the message into an Amazon RDS database.

Answer: B

Question #129

An advertising company has a dynamic website with heavy traffic. The company wants to migrate the website infrastructure to AWS to handle everything except website development.

Which solution BEST meets these requirements?

- A. Use AWS VM Import to migrate a web server image to AWS. Launch the image on a compute-optimized Amazon EC2 instance.
- B. Launch multiple Amazon Lightsail instances behind a load balancer. Set up the website on those instances.
- C. Deploy the website code in an AWS Elastic Beanstalk environment. Use Auto Scaling to scale the numbers of instances.
- D. Use Amazon S3 to host the website. Use Amazon CloudFront to deliver the content at scale.

Answer: C

Reference:

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

Question #130

A Software Engineer developed an AWS Lambda function in Node.js to do some CPU-intensive data processing. With the default settings, the Lambda function takes about 5 minutes to complete.

Which approach should a Developer take to increase the speed of completion?

- A. Instead of using Node.js, rewrite the Lambda function using Python.

<https://itexamcertified.com>

<https://itexamcertified.com>

- B. Instead of packaging the libraries in the ZIP file with the function, move them to a Lambda layer and use the layer with the function.
- C. Allocate the maximum available CPU units to the function.
- D. Increase the available memory to the function.

Answer: D

Reference:

<https://serverless.zone/my-accidental-3-5x-speed-increase-of-aws-lambda-functions-6d95351197f3>

Question #131

A company has implemented AWS CodePipeline to automate its release pipelines. The Development team is writing an AWS Lambda function what will send notifications for state changes of each of the actions in the stages.

Which steps must be taken to associate the Lambda function with the event source?

- A. Create a trigger that invokes the Lambda function from the Lambda console by selecting CodePipeline as the event source.
- B. Create an event trigger and specify the Lambda function from the CodePipeline console.
- C. Create an Amazon CloudWatch alarm that monitors status changes in Code Pipeline and triggers the Lambda function.
- D. Create an Amazon CloudWatch Events rule that uses CodePipeline as an event source.

Answer: D

Reference:

<https://aws.amazon.com/blogs/devops/using-aws-step-functions-state-machines-to-handle-workflow-driven-aws-codepipeline-actions/>

Question #132

A Developer has built an application running on AWS Lambda using AWS Serverless Application Model (AWS SAM).

What is the correct order of execution to successfully deploy the application?

- A. 1. Build the SAM template in Amazon EC2. 2. Package the SAM template to Amazon EBS storage. 3. Deploy the SAM template from Amazon EBS.
- B. 1. Build the SAM template locally. 2. Package the SAM template onto Amazon S3. 3. Deploy the SAM template from Amazon S3.
- C. 1. Build the SAM template locally. 2. Deploy the SAM template from Amazon S3. 3. Package the SAM template for use.

<https://itexamcertified.com>

<https://itexamcertified.com>

D. 1. Build the SAM template locally. 2. Package the SAM template from AWS CodeCommit. 3. Deploy the SAM template to CodeCommit.

Answer: B

Reference:

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-deploying.html>

Question #133

A company wants to migrate an imaging service to Amazon EC2 while following security best practices. The images are sourced and read from a non-public

Amazon S3 bucket.

What should a Developer do to meet these requirements?

- A. Create an IAM user with read-only permissions for the S3 bucket. Temporarily store the user credentials in the Amazon EBS volume of the EC2 instance.
- B. Create an IAM user with read-only permissions for the S3 bucket. Temporarily store the user credentials in the user data of the EC2 instance.
- C. Create an EC2 service role with read-only permissions for the S3 bucket. Attach the role to the EC2 instance.
- D. Create an S3 service role with read-only permissions for the S3 bucket. Attach the role to the EC2 instance.

Answer: B

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

Question #134

A Development team wants to immediately build and deploy an application whenever there is a change to the source code.

Which approaches could be used to trigger the deployment? (Choose two.)

- A. Store the source code in an Amazon S3 bucket. Configure AWS CodePipeline to start whenever a file in the bucket changes.
- B. Store the source code in an encrypted Amazon EBS volume. Configure AWS CodePipeline to start whenever a file in the volume changes.
- C. Store the source code in an AWS CodeCommit repository. Configure AWS CodePipeline to start whenever a change is committed to the repository.
- D. Store the source code in an Amazon S3 bucket. Configure AWS CodePipeline to start every 15 minutes.

<https://itexamcertified.com>

<https://itexamcertified.com>

E. Store the source code in an Amazon EC2 instance's ephemeral storage. Configure the instance to start AWS CodePipeline whenever there are changes to the source code.

Answer: AC

Reference:

<https://docs.aws.amazon.com/codepipeline/latest/userguide/tutorials-ecs-ecr-codedeploy.html>

Question #135

A company has implemented AWS CodeDeploy as part of its cloud native CI/CD stack. The company enables automatic rollbacks while deploying a new version of a popular web application from in-place to Amazon EC2.

What occurs if the deployment of the new version fails due to code regression?

- A. The last known good deployment is automatically restored using the snapshot stored in Amazon S3.
- B. CodeDeploy switches the Amazon Route 53 alias records back to the known good green deployment and terminates the failed blue deployment.
- C. A new deployment of the last known version of the application is deployed with a new deployment ID.
- D. AWS CodePipeline promotes the most recent deployment with a SUCCEEDED status to production.

Answer: C

Question #136

A software company needs to make sure user-uploaded documents are securely stored in Amazon S3. The documents must be encrypted at rest in Amazon S3.

The company does not want to manage the security infrastructure in-house, but the company still needs extra protection to ensure it has control over its encryption keys due to industry regulations.

Which encryption strategy should a Developer use to meet these requirements?

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

Answer: B

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

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

Question #137

A Developer uses Amazon S3 buckets for static website hosting. The Developer creates one S3 bucket for the code and another S3 bucket for the assets, such as image and video files. Access is denied when a user attempts to access the assets bucket from the code bucket, with the website application showing a 403 error.

How should the Developer solve this issue?

- A. Create an IAM role and apply it to the assets bucket for the code bucket to be granted access.
- B. Edit the bucket policy of the assets bucket to open access to all principals.
- C. Edit the cross-origin resource sharing (CORS) configuration of the assets bucket to allow any origin to access the assets.
- D. Change the code bucket to use AWS Lambda functions instead of static website hosting.

Answer: C

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/static-website-hosting.html>

Question #138

A Developer migrated a web application to AWS. As part of the migration, the Developer implemented an automated continuous integration/continuous improvement (CI/CD) process using a blue/green deployment. The deployment provisions new Amazon EC2 instances in an Auto Scaling group behind a new

Application Load Balancer. After the migration was completed, the Developer began receiving complaints from users getting booted out of the system. The system also requires users to log in after every new deployment.

How can these issues be resolved?

- A. Use rolling updates instead of a blue/green deployment
- B. Externalize the user sessions to Amazon ElastiCache
- C. Turn on sticky sessions in the Application Load Balancer
- D. Use multicast to replicate session information

Answer: B

Question #139

<https://itexamcertified.com>

<https://itexamcertified.com>

A Developer wants to insert a record into an Amazon DynamoDB table as soon as a new file is added to an Amazon S3 bucket.

Which set of steps would be necessary to achieve this?

- A. Create an event with Amazon CloudWatch Events that will monitor the S3 bucket and then insert the records into DynamoDB.
- B. Configure an S3 event to invoke a Lambda function that inserts records into DynamoDB.
- C. Create a Lambda function that will poll the S3 bucket and then insert the records into DynamoDB.
- D. Create a cron job that will run at a scheduled time and insert the records into DynamoDB.

Answer: B

Question #140

A Developer is building an application that needs to store data in Amazon S3. Management requires that the data be encrypted before it is sent to Amazon S3 for storage. The encryption keys need to be managed by the Security team.

Which approach should the Developer take to meet these requirements?

- A. Implement server-side encryption using customer-provided encryption keys (SSE-C).
- B. Implement server-side encryption by using a client-side master key.
- C. Implement client-side encryption using an AWS KMS managed customer master key (CMK).
- D. Implement client-side encryption using Amazon S3 managed keys.

Answer: C

Reference:

<https://aws.amazon.com/s3/faqs/>

Question #141

A Developer has written an Amazon Kinesis Data Streams application. As usage grows and traffic increases over time, the application is regularly receiving

ProvisionedThroughputExceededException error messages.

Which steps should the Developer take to resolve the error? (Choose two.)

- A. Use Auto Scaling to scale the stream for better performance
- B. Increase the delay between the GetRecords call and the PutRecords call

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. Increase the number of shards in the data stream
- D. Specify a shard iterator using the ShardIterator parameter
- E. Implement exponential backoff on the GetRecords call and the PutRecords call

Answer: CE

Reference:

<https://docs.aws.amazon.com/streams/latest/dev/troubleshooting-consumers.html>

Question #142

A Developer is publishing critical log data to a log group in Amazon CloudWatch Logs, which was created 2 months ago. The Developer must encrypt the log data using an AWS KMS customer master key (CMK) so future data can be encrypted to comply with the company's security policy.

How can the Developer meet this requirement?

- A. Use the CloudWatch Logs console and enable the encrypt feature on the log group
- B. Use the AWS CLI create-log-group command and specify the key Amazon Resource Name (ARN)
- C. Use the KMS console and associate the CMK with the log group
- D. Use the AWS CLI associate-kms-key command and specify the key Amazon Resource Name (ARN)

Answer: D

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/encrypt-log-data-kms.html>

Question #143

A Developer has code running on Amazon EC2 instances that needs read-only access to an Amazon DynamoDB table.

What is the MOST secure approach the Developer should take to accomplish this task?

- A. Create a user access key for each EC2 instance with read-only access to DynamoDB. Place the keys in the code. Redeploy the code as keys rotate.
- B. Use an IAM role with an AmazonDynamoDBReadOnlyAccess policy applied to the EC2 instances.
- C. Run all code with only AWS account root user access keys to ensure maximum access to services.
- D. Use an IAM role with Administrator access applied to the EC2 instance.

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: B

Question #144

A Developer decides to store highly secure data in Amazon S3 and wants to implement server-side encryption (SSE) with granular control of who can access the master key. Company policy requires that the master key be created, rotated, and disabled easily when needed, all for security reasons.

Which solution should be used to meet these requirements?

- A. SSE with Amazon S3 managed keys (SSE-S3)
- B. SSE with AWS KMS managed keys (SSE-KMS)
- C. SSE with AWS Secrets Manager
- D. SSE with customer-provided encryption keys

Answer: B

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

Question #145

A Developer is migrating an on-premises application to AWS. The application currently takes user uploads and saves them to a local directory on the server. All uploads must be saved and made immediately available to all instances in an Auto Scaling group.

Which approach will meet these requirements?

- A. Use Amazon EBS and configure the application AMI to use a snapshot of the same EBS instance on boot.
- B. Use Amazon S3 and rearchitect the application so all uploads are placed in S3.
- C. Use instance storage and share it between instances launched from the same Amazon Machine Image (AMI).
- D. Use Amazon EBS and file synchronization software to achieve eventual consistency among the Auto Scaling group.

Answer: B

Question #146

A Developer implemented a static website hosted in Amazon S3 that makes web service requests hosted in Amazon API Gateway and AWS Lambda. The site is showing an error that reads: "No 'Access-Control-Allow-Origin' header is present on the requested resource. Origin 'null' is therefore not allowed access."

<https://itexamcertified.com>

<https://itexamcertified.com>

What should the Developer do to resolve this issue?

- A. Enable cross-origin resource sharing (CORS) on the S3 bucket.
- B. Enable cross-origin resource sharing (CORS) for the method in API Gateway
- C. Add the Access-Control-Request-Method header to the request
- D. Add the Access-Control-Request-Headers header to the request

Answer: B

Reference:

<https://forums.aws.amazon.com/thread.jspa?threadID=252972>

Question #147

A Developer is writing an application in AWS Lambda. To simplify testing and deployments, the Developer needs the database connections string to be easily changed without modifying the Lambda code.

How can this requirement be met?

- A. Store the connection string as a secret in AWS Secrets Manager.
- B. Store the connection string in an IAM user account.
- C. Store the connection string in AWS KMS.
- D. Store the connection string as a Lambda layer.

Answer: A

Reference:

<https://aws.amazon.com/blogs/developer/net-core-configuration-provider-for-aws-systems-manager/>

Question #148

A company is launching an ecommerce website and will host the static data in Amazon S3. The company expects approximately 1,000 transactions per second

(TPS) for GET and PUT requests in total. Logging must be enabled to track all requests and must be retained for auditing purposes.

What is the MOST cost-effective solution?

- A. Enable AWS CloudTrail logging for the S3 bucket-level action and create a lifecycle policy to move the data from the log bucket to Amazon S3 Glacier in 90 days.
- B. Enable S3 server access logging and create a lifecycle policy to expire the data in 90 days.

<https://itexamcertified.com>

<https://itexamcertified.com>

C. Enable AWS CloudTrail logging for the S3 bucket-level action and create a lifecycle policy to expire the data in 90 days.

D. Enable S3 server access logging and create a lifecycle policy to move the data to Amazon S3 Glacier in 90 days.

Answer: D

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-request-identification.html>

Question #149

A company is building a compute-intensive application that will run on a fleet of Amazon EC2 instances. The application uses attached Amazon EBS disks for storing data. The application will process sensitive information and all the data must be encrypted.

What should a Developer do to ensure the data is encrypted on disk without impacting performance?

- A. Configure the Amazon EC2 instance fleet to use encrypted EBS volumes for storing data.
- B. Add logic to write all data to an encrypted Amazon S3 bucket.
- C. Add a custom encryption algorithm to the application that will encrypt and decrypt all data.
- D. Create a new Amazon Machine Image (AMI) with an encrypted root volume and store the data to ephemeral disks.

Answer: A

Reference:

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

Question #150

A Developer has written an application that runs on Amazon EC2 instances and generates a value every minute. The Developer wants to monitor and graph the values generated over time without logging in to the instance each time.

Which approach should the Developer use to achieve this goal?

- A. Use the Amazon CloudWatch metrics reported by default for all EC2 instances. View each value from the CloudWatch console.
- B. Develop the application to store each value in a file on Amazon S3 every minute with the timestamp as the name.

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. Publish each generated value as a custom metric to Amazon CloudWatch using available AWS SDKs.
- D. Store each value as a variable and add the variable to the list of EC2 metrics that should be reported to the Amazon CloudWatch console.

Answer: C

Question #151

A Development team decides to adopt a continuous integration/continuous delivery (CI/CD) process using AWS CodePipeline and AWS CodeCommit for a new application. However, management wants a person to review and approve the code before it is deployed to production.

How can the Development team add a manual approver to the CI/CD pipeline?

- A. Use AWS SES to send an email to approvers when their action is required. Develop a simple application that allows approvers to accept or reject a build. Invoke an AWS Lambda function to advance the pipeline when a build is accepted.
- B. If approved, add an approved tag when pushing changes to the CodeCommit repository. CodePipeline will proceed to build and deploy approved commits without interruption.
- C. Add an approval step to CodeCommit. Commits will not be saved until approved.
- D. Add an approval action to the pipeline. Configure the approval action to publish to an Amazon SNS topic when approval is required. The pipeline execution will stop and wait for an approval.

Answer: D

Reference:

<https://docs.aws.amazon.com/codepipeline/latest/userguide/approvals-action-add.html>

Question #152

A Developer is building a serverless application using AWS Lambda and must create a REST API using an HTTP GET method.

What needs to be defined to meet this requirement? (Choose two.)

- A. A Lambda@Edge function
- B. An Amazon API Gateway with a Lambda function
- C. An exposed GET method in an Amazon API Gateway
- D. An exposed GET method in the Lambda function
- E. An exposed GET method in Amazon Route 53

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: BC

Reference:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-getting-started-with-rest-apis.html>

Question #153

A Developer needs to create an application that supports Security Assertion Markup Language (SAML) and Facebook authentication. It must also allow access to

AWS services, such as Amazon DynamoDB.

Which AWS service or feature will meet these requirements with the LEAST amount of additional coding?

- A. AWS AppSync
- B. Amazon Cognito identity pools
- C. Amazon Cognito user pools
- D. Amazon Lambda@Edge

Answer: B

Reference:

<https://aws.amazon.com/blogs/mobile/amazon-cognito-user-pools-supports-federation-with-saml/>

Question #154

A Developer is trying to monitor an application's status by running a cron job that returns 1 if the service is up and 0 if the service is down. The Developer created code that uses an AWS CLI put-metric-alarm command to publish the custom metrics to Amazon CloudWatch and create an alarm. However, the Developer is unable to create an alarm as the custom metrics do not appear in the CloudWatch console.

What is causing this issue?

- A. Sending custom metrics using the CLI is not supported.
- B. The Developer needs to use the put-metric-data command.
- C. The Developer must use a unified CloudWatch agent to publish custom metrics.
- D. The code is not running on an Amazon EC2 instance.

Answer: B

Question #155

<https://itexamcertified.com>

<https://itexamcertified.com>

A Developer registered an AWS Lambda function as a target for an Application Load Balancer (ALB) using a CLI command. However, the Lambda function is not being invoked when the client sends requests through the ALB.

Why is the Lambda function not being invoked?

- A. A Lambda function cannot be registered as a target for an ALB.
- B. A Lambda function can be registered with an ALB using AWS Management Console only.
- C. The permissions to invoke the Lambda function are missing.
- D. Cross-zone is not enabled on the ALB.

Answer: C

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/lambda-functions.html>

Question #156

A company provides APIs as a service and commits to a service level agreement (SLA) with all its users.

To comply with each SLA, what should the company do?

- A. Enable throttling limits for each method in Amazon API Gateway
- B. Create a usage plan for each user and request API keys to access the APIs
- C. Enable API rate limiting in Amazon Cognito for each user
- D. Enable default throttling limits for each stage after deploying the APIs

Answer: B

Question #157

A Developer is preparing a deployment package using AWS CloudFormation. The package consists of two separate templates: one for the infrastructure and one for the application. The application has to be inside the VPC that is created from the infrastructure template.

How can the application stack refer to the VPC created from the infrastructure template?

- A. Use the Ref function to import the VPC into the application stack from the infrastructure template.
- B. Use the export flag in the infrastructure template, and then use the Fn::ImportValue function in the application template.
- C. Use the DependsOn attribute to specify that the application instance depends on the VPC in the application template.

<https://itexamcertified.com>

<https://itexamcertified.com>

D. Use the Fn::GetAtt function to include the attribute of the VPC in the application template.

Answer: B

Question #158

A Developer must allow guest users without logins to access an Amazon Cognito-enabled site to view files stored within an Amazon S3 bucket.

How should the Developer meet these requirements?

- A. Create a blank user ID in a user pool, add to the user group, and grant access to AWS resources.
- B. Create a new identity pool, enable access to authenticated identities, and grant access to AWS resources.
- C. Create a new user pool, enable access to authenticated identities, and grant access to AWS resources.
- D. Create a new user pool, disable authentication access, and grant access to AWS resources.

Answer: B

Question #159

A Developer has written code for an application and wants to share it with other Developers on the team to receive feedback. The shared application code needs to be stored long-term with multiple versions and batch change tracking.

Which AWS service should the Developer use?

- A. AWS CodeBuild
- B. Amazon S3
- C. AWS CodeCommit
- D. AWS Cloud9

Answer: C

Reference:

<https://docs.aws.amazon.com/codecommit/latest/userguide/codecommit-user.pdf>

Question #160

<https://itexamcertified.com>

<https://itexamcertified.com>

A Developer has discovered that an application responsible for processing messages in an Amazon SQS queue is routinely falling behind. The application is capable of processing multiple messages in one execution, but is only receiving one message at a time.

What should the Developer do to increase the number of messages the application receives?

- A. Call the ChangeMessageVisibility API for the queue and set MaxNumberOfMessages to a value greater than the default of 1.
- B. Call the AddPermission API to set MaxNumberOfMessages for the ReceiveMessage action to a value greater than the default of 1.
- C. Call the ReceiveMessage API to set MaxNumberOfMessages to a value greater than the default of 1.
- D. Call the SetQueueAttributes API for the queue and set MaxNumberOfMessages to a value greater than the default of 1.

Answer: C

Reference:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_ReceiveMessage.html

Question #161

A Developer is investigating an application's performance issues. The application consists of hundreds of microservices, and a single API call can potentially have a deep call stack. The Developer must isolate the component that is causing the issue.

Which AWS service or feature should the Developer use to gather information about what is happening and isolate the fault?

- A. AWS X-Ray
- B. VPC Flow Logs
- C. Amazon GuardDuty
- D. Amazon Macie

Answer: A

Question #162

A Company runs continuous integration/continuous delivery (CI/CD) pipelines for its application on AWS CodePipeline. A Developer must write unit tests and run them as part of the pipelines before staging the artifacts for testing.

How should the Developer incorporate unit tests as part of CI/CD pipelines?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Create a separate CodePipeline pipeline to run unit tests
- B. Update the AWS CodeBuild specification to include a phase for running unit tests
- C. Install the AWS CodeDeploy agent on an Amazon EC2 instance to run unit tests
- D. Create a testing branch in AWS CodeCommit to run unit tests

Answer: B

Question #163

An application has the following requirements:

- Performance efficiency of seconds with up to a minute of latency.
- The data storage size may grow up to thousands of terabytes.
- Per-message sizes may vary between 100 KB and 100 MB.
- Data can be stored as key/value stores supporting eventual consistency.

What is the MOST cost-effective AWS service to meet these requirements?

- A. Amazon DynamoDB
- B. Amazon S3
- C. Amazon RDS (with a MySQL engine)
- D. Amazon ElastiCache

Answer: B

Reference:

<https://aws.amazon.com/nosql/key-value/>

Question #164

An application is experiencing performance issues based on increased demand. This increased demand is on read-only historical records pulled from an Amazon

RDS-hosted database with custom views and queries. A Developer must improve performance without changing the database structure.

Which approach will improve performance and MINIMIZE management overhead?

- A. Deploy Amazon DynamoDB, move all the data, and point to DynamoDB.
- B. Deploy Amazon ElastiCache for Redis and cache the data for the application.

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. Deploy Memcached on Amazon EC2 and cache the data for the application.
- D. Deploy Amazon DynamoDB Accelerator (DAX) on Amazon RDS to improve cache performance.

Answer: B

Question #165

A Developer has an Amazon DynamoDB table that must be in provisioned mode to comply with user requirements. The application needs to support the following:

- ➡ Average item size: 10 KB
- ➡ Item reads each second: 10 strongly consistent
- ➡ Item writes each second: 2 transactional

Which read and write capacity cost-effectively meets these requirements?

- A. Read 10; write 2
- B. Read 30; write 40
- C. Use on-demand scaling
- D. Read 300; write 400

Answer: D

Question #166

A company wants to containerize an existing three-tier web application and deploy it to Amazon ECS Fargate. The application is using session data to keep track of user activities.

Which approach would provide the BEST user experience?

- A. Provision a Redis cluster in Amazon ElastiCache and save the session data in the cluster.
- B. Create a session table in Amazon Redshift and save the session data in the database table.
- C. Enable session stickiness in the existing Network Load Balancer and manage the session data in the container.
- D. Use an Amazon S3 bucket as data store and save the session data in the bucket.

Answer: A

Question #167

<https://itexamcertified.com>

<https://itexamcertified.com>

An application is using a single-node Amazon ElastiCache for Redis instance to improve read performance. Over time, demand for the application has increased exponentially, which has increased the load on the ElastiCache instance. It is critical that this cache layer handles the load and is resilient in case of node failures.

What can the Developer do to address the load and resiliency requirements?

- A. Add a read replica instance.
- B. Migrate to a Memcached cluster.
- C. Migrate to an Amazon Elasticsearch Service cluster.
- D. Vertically scale the ElastiCache instance.

Answer: A

Reference:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Replication.Redis.Groups.html>

Question #168

A Developer is designing an AWS Lambda function that creates temporary files that are less than 10 MB during execution. The temporary files will be accessed and modified multiple times during execution. The Developer has no need to save or retrieve these files in the future.

Where should the temporary file be stored?

- A. the /tmp directory
- B. Amazon EFS
- C. Amazon EBS
- D. Amazon S3

Answer: A

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-dg.pdf>

(23)

Question #169

A Developer is writing an application that runs on Amazon EC2 instances in an Auto Scaling group. The application data is stored in an Amazon DynamoDB table and records are constantly updated by all instances. An instance sometimes retrieves old data. The Developer wants to correct this by making sure the reads are strongly consistent.

<https://itexamcertified.com>

<https://itexamcertified.com>

How can the Developer accomplish this?

- A. Set ConsistentRead to true when calling GetItem.
- B. Create a new DynamoDB Accelerator (DAX) table.
- C. Set Consistency to strong when calling UpdateTable.
- D. Use the GetShardIterator command.

Answer: A

Reference:

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

Question #170

A Developer has an application that must accept a large amount of incoming data streams and process the data before sending it to many downstream users.

Which serverless solution should the Developer use to meet these requirements?

- A. Amazon RDS MySQL stored procedure with AWS Lambda
- B. AWS Direct Connect with AWS Lambda
- C. Amazon Kinesis Data Streams with AWS Lambda
- D. Amazon EC2 bash script with AWS Lambda

Answer: C

Reference:

<https://aws.amazon.com/kinesis/data-analytics/faqs/>

Question #171

A company is using Amazon API Gateway to manage its public-facing API. The CISO requires that the APIs be used by test account users only.

What is the MOST secure way to restrict API access to users of this particular AWS account?

- A. Client-side SSL certificates for authentication
- B. API Gateway resource policies
- C. Cross-origin resource sharing (CORS)
- D. Usage plans

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: B

Reference:

<https://aws.amazon.com/blogs/compute/control-access-to-your-apis-using-amazon-api-gateway-resource-policies/>

Question #172

A Developer is migrating existing applications to AWS. These applications use MongoDB as their primary data store, and they will be deployed to Amazon EC2 instances. Management requires that the Developer minimize changes to applications while using AWS services.

Which solution should the Developer use to host MongoDB in AWS?

- A. Install MongoDB on the same instance where the application is running.
- B. Deploy Amazon DocumentDB in MongoDB compatibility mode.
- C. Use Amazon API Gateway to translate API calls from MongoDB to Amazon DynamoDB.
- D. Replicate the existing MongoDB workload to Amazon DynamoDB.

Answer: D

Question #173

A company requires that AWS Lambda functions written by Developers log errors so System Administrators can more effectively troubleshoot issues.

What should the Developers implement to meet this need?

- A. Publish errors to a dedicated Amazon SQS queue.
- B. Create an Amazon CloudWatch Events event trigger based on certain Lambda events.
- C. Report errors through logging statements in Lambda function code.
- D. Set up an Amazon SNS topic that sends logging statements upon failure.

Answer: B

Question #174

A Developer needs to deploy an application running on AWS Fargate using Amazon ECS. The application has environment variables that must be passed to a container for the application to initialize.

<https://itexamcertified.com>

<https://itexamcertified.com>

How should the environment variables be passed to the container?

- A. Define an array that includes the environment variables under the environment parameter within the service definition.
- B. Define an array that includes the environment variables under the environment parameter within the task definition.
- C. Define an array that includes the environment variables under the entryPoint parameter within the task definition.
- D. Define an array that includes the environment variables under the entryPoint parameter within the service definition.

Answer: B

Question #175

A company's fleet of Amazon EC2 instances receives data from millions of users through an API. The servers batch the data, add an object for each user, and upload the objects to an S3 bucket to ensure high access rates. The object attributes are Customer ID, Server ID, TS-Server (TimeStamp and Server ID), the size of the object, and a timestamp. A Developer wants to find all the objects for a given user collected during a specified time range.

After creating an S3 object created event, how can the Developer achieve this requirement?

- A. Execute an AWS Lambda function in response to the S3 object creation events that creates an Amazon DynamoDB record for every object with the Customer ID as the partition key and the Server ID as the sort key. Retrieve all the records using the Customer ID and Server ID attributes.
- B. Execute an AWS Lambda function in response to the S3 object creation events that creates an Amazon Redshift record for every object with the Customer ID as the partition key and TS-Server as the sort key. Retrieve all the records using the Customer ID and TS-Server attributes.
- C. Execute an AWS Lambda function in response to the S3 object creation events that creates an Amazon DynamoDB record for every object with the Customer ID as the partition key and TS-Server as the sort key. Retrieve all the records using the Customer ID and TS-Server attributes.
- D. Execute an AWS Lambda function in response to the S3 object creation events that creates an Amazon Redshift record for every object with the Customer ID as the partition key and the Server ID as the sort key. Retrieve all the records using the Customer ID and Server ID attributes.

Answer: C

Question #176

A company is managing a NoSQL database on-premises to host a critical component of an application, which is starting to have scaling issues. The company wants to migrate the application to Amazon DynamoDB with the following considerations:

<https://itexamcertified.com>

<https://itexamcertified.com>

- ➡ Optimize frequent queries
- ➡ Reduce read latencies
- ➡ Plan for frequent queries on certain key attributes of the table

Which solution would help achieve these objectives?

- A. Create global secondary indexes on keys that are frequently queried. Add the necessary attributes into the indexes.
- B. Create local secondary indexes on keys that are frequently queried. DynamoDB will fetch needed attributes from the table.
- C. Create DynamoDB global tables to speed up query responses. Use a scan to fetch data from the table.
- D. Create an AWS Auto Scaling policy for the DynamoDB table.

Answer: A

Question #177

A developer is writing an application that will process data delivered into an Amazon S3 bucket. The data is delivered approximately 10 times a day, and the developer expects the data will be processed in less than 1 minute, on average.

How can the developer deploy and invoke the application with the lowest cost and lowest latency?

- A. Deploy the application as an AWS Lambda function and invoke it with an Amazon CloudWatch alarm triggered by an S3 object upload.
- B. Deploy the application as an AWS Lambda function and invoke it with an S3 event notification.
- C. Deploy the application as an AWS Lambda function and invoke it with an Amazon CloudWatch scheduled event.
- D. Deploy the application onto an Amazon EC2 instance and have it poll the S3 bucket for new objects.

Answer: B

Reference:

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

Question #178

A developer converted an existing program to an AWS Lambda function in the console. The program runs properly on a local laptop, but shows an "Unable to import module" error when tested in the Lambda console.

Which of the following can fix the error?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Install the missing module and specify the current directory as the target. Create a ZIP file to include all files under the current directory, and upload the ZIP file.
- B. Install the missing module in a lib directory. Create a ZIP file to include all files under the lib directory, and upload the ZIP file as dependency file.
- C. In the Lambda code, invoke a Linux command to install the missing modules under the /usr/lib directory.
- D. In the Lambda console, create a LB_LIBRARY_PATH environment and specify the value for the system library plan.

Answer: B

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-dg.pdf>

Question #179

A front-end web application is using Amazon Cognito user pools to handle the user authentication flow. A developer is integrating Amazon DynamoDB into the application using the AWS SDK for JavaScript.

How would the developer securely call the API without exposing the access or secret keys?

- A. Configure Amazon Cognito identity pools and exchange the JSON Web Token (JWT) for temporary credentials.
- B. Run the web application in an Amazon EC2 instance with the instance profile configured.
- C. Hardcore the credentials, use Amazon S3 to host the web application, and enable server-side encryption.
- D. Use Amazon Cognito user pool JSON Web Tokens (JWITs) to access the DynamoDB APIs.

Answer: A

Reference:

<https://docs.aws.amazon.com/cognito/latest/developerguide/amazon-cognito-user-pools-using-tokens-verifying-a-jwt.html>

Question #180

A developer needs to manage AWS infrastructure as code and must be able to deploy multiple identical copies of the infrastructure, stage changes, and revert to previous versions.

Which approach addresses these requirements?

- A. Use cost allocation reports and AWS OpsWorks to deploy and manage the infrastructure.
- B. Use Amazon CloudWatch metrics and alerts along with resource tagging to deploy and manage the infrastructure.

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. Use AWS Elastic Beanstalk and AWS CodeCommit to deploy and manage the infrastructure.
- D. Use AWS CloudFormation and AWS CodeCommit to deploy and manage the infrastructure.

Answer: D

Question #181

What is required to trace Lambda-based applications with AWS X-Ray?

- A. Send logs from the Lambda application to an S3 bucket; trigger a Lambda function from the bucket to send data to AWS X-Ray.
- B. Trigger a Lambda function from the application logs in Amazon CloudWatch to submit tracing data to AWS X-Ray.
- C. Use an IAM execution role to give the Lambda function permissions and enable tracing.
- D. Update and add AWS X-Ray daemon code to relevant parts of the Lambda function to set up the trace.

Answer: C

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/services-xray.html>

Question #182

A development team is building a new application that will run on Amazon EC2 and use Amazon DynamoDB as a storage layer. The developers all have assigned

IAM user accounts in the same IAM group. The developers currently can launch EC2 instances, and they need to be able to launch EC2 instances with an instance role allowing access to Amazon DynamoDB.

Which AWS IAM changes are needed when creating an instance role to provide this functionality?

- A. Create an IAM permission policy attached to the role that allows access to DynamoDB. Add a trust policy to the role that allows DynamoDB to assume the role. Attach a permissions policy to the development group in AWS IAM that allows developers to use the iam:GetRole and iam:PassRole permissions for the role.
- B. Create an IAM permissions policy attached to the role that allows access to DynamoDB. Add a trust policy to the role that allows Amazon EC2 to assume the role. Attach a permissions policy to the development group in AWS IAM that allows developers to use the iam:PassRole permission for the role.
- C. Create an IAM permission policy attached to the role that allows access to Amazon EC2. Add a trust policy to the role that allows DynamoDB to assume the role. Attach a permissions policy to the development group in AWS IAM that allows developers to use the iam:PassRole permission for the role.

<https://itexamcertified.com>

D. Create an IAM permissions policy attached to the role that allows access to DynamoDB. Add a trust policy to the role that allows Amazon EC2 to assume the role. Attach a permissions policy to the development group in AWS IAM that allows developers to use the iam:GetRole permission for the role.

Answer: B

Reference:

<https://docs.aws.amazon.com/glue/latest/dg/attach-policy-iam-user.html>

Question #183

A developer is migrating code to an AWS Lambda function that will an Amazon Aurora MySQL database.

What is the MOST secure way to authenticate the function to the database?

- A. Store the database credentials as encrypted parameters in AWS Systems Manager Parameters Store. Obtain the credentials from Systems Manager when the Lambda function needs to connect to the database.
- B. Store the database credentials in AWS Secrets Manager. Let Secrets Manager handle the rotation of the credentials, as required.
- C. Store the database credentials in an Amazon S3 bucket that has a restrictive bucket policy for the Lambda role when accessing the credentials. Use AWS KMS to encrypt the data.
- D. Create a policy with rds-db:connect access to the database and attach it to the role assigned to the Lambda function.

Answer: B

Reference:

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>

Question #184

A development team uses AWS Elastic Beanstalk for application deployment. The team has configured the application version lifecycle policy to limit the number of application versions to 25. However, even with the lifecycle policy, the source bundle is deleted from the Amazon S3 source bucket.

What should a developer do in the Elastic Beanstalk application version lifecycle settings to retain the source code in the S3 bucket?

- A. Change the Set the application versions limit by total count setting to zero.
- B. Disable the Lifecycle policy setting.
- C. Change the Set the application version limit by age setting to zero.

<https://itexamcertified.com>

D. Set Retention to Retain source bundle in S3.

Answer: D

Reference:

<https://digitalcloud.training/certification-training/aws-developer-associate/aws-compute/elastic-beanstalk/>

Question #185

A developer has built a market application that stores pricing data in Amazon DynamoDB with Amazon ElastiCache in front. The prices of items in the market change frequently. Sellers have begun complaining that, after they update the price of an item, the price does not actually change in the product listing.

What could be causing this issue?

- A. The cache is not being invalidated when the price of the item is changed
- B. The price of the item is being retrieved using a write-through ElastiCache cluster
- C. The DynamoDB table was provisioned with insufficient read capacity
- D. The DynamoDB table was provisioned with insufficient write capacity

Answer: A

Question #186

A developer is provided with an HTTPS clone URL for an AWS CodeCommit repository.

What needs to be configured before cloning this repository?

- A. Use AWS KMS to set up public and private keys for use with AWS CodeCommit.
- B. Set up the Git credential helper to use an AWS credential profile, and enable the helper to send the path to the repositories.
- C. Use AWS Certificate Manager to provision public and private SSL/TLS certificates.
- D. Generate encryption keys using AWS CloudHSM, then export the key for use with AWS CodeCommit.

Answer: B

AWS credential profile, and enabling the Git credential helper to send the path to repositories:

Reference:

<https://docs.aws.amazon.com/codecommit/latest/userguide/setting-up-https-unixes.html>

<https://itexamcertified.com>

Question #187

A developer is building an application using an Amazon API Gateway REST API backend by an AWS Lambda function that interacts with an Amazon DynamoDB table. During testing, the developer observes high latency when making requests to the API.

How can the developer evaluate the end-to-end latency and identify performance bottlenecks?

- A. Enable AWS CloudTrail logging and use the logs to map each latency and bottleneck.
- B. Enable and configure AWS X-Ray tracing on API Gateway and the Lambda function. Use X-Ray to trace and analyze user requests.
- C. Enable Amazon CloudWatch Logs for the Lambda function. Enable execution logs for API Gateway to view and analyze user request logs.
- D. Enable VPC Flow Logs to capture and analyze network traffic within the VPC.

Answer: B

Reference:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-xray.html>

Question #188

A developer is writing an AWS Lambda function. The developer wants to log key events that occur during the Lambda function and include a unique identifier to associate the events with a specific function invocation.

Which of the following will help the developer accomplish this objective?

- A. Obtain the request identifier from the Lambda context object. Architect the application to write logs to the console.
- B. Obtain the request identifier from the Lambda event object. Architect the application to write logs to a file.
- C. Obtain the request identifier from the Lambda event object. Architect the application to write logs to the console.
- D. Obtain the request identifier from the Lambda context object. Architect the application to write logs to a file.

Answer: A

Question #189

An IAM role is attached to an Amazon EC2 instance that explicitly denies access to all Amazon S3 API actions. The EC2 instance credentials file specifies the IAM access key and secret access key, which allow full administrative access.

Given that multiple modes of IAM access are present for this EC2 instance, which of the following is correct?

<https://itexamcertified.com>

- A. The EC2 instance will only be able to list the S3 buckets.
- B. The EC2 instance will only be able to list the contents of one S3 bucket at a time.
- C. The EC2 instance will be able to perform all actions on any S3 bucket.
- D. The EC2 instance will not be able to perform any S3 action on any S3 bucket.

Answer: C

Question #190

Two containerized microservices are hosted on Amazon EC2 ECS. The first microservice reads an Amazon RDS Aurora database instance, and the second microservice reads an Amazon DynamoDB table.

How can each microservice be granted the minimum privileges?

- A. Set ECS_ENABLE_TASK_IAM_ROLE to false on EC2 instance boot in ECS agent configuration file. Run the first microservice with an IAM role for ECS tasks with read-only access for the Aurora database. Run the second microservice with an IAM role for ECS tasks with read-only access to DynamoDB.
- B. Set ECS_ENABLE_TASK_IAM_ROLE to false on EC2 instance boot in the ECS agent configuration file. Grant the instance profile role read-only access to the Aurora database and DynamoDB.
- C. Set ECS_ENABLE_TASK_IAM_ROLE to true on EC2 instance boot in the ECS agent configuration file. Run the first microservice with an IAM role for ECS tasks with read-only access for the Aurora database. Run the second microservice with an IAM role for ECS tasks with read-only access to DynamoDB.
- D. Set ECS_ENABLE_TASK_IAM_ROLE to true on EC2 instance boot in the ECS agent configuration file. Grant the instance profile role read-only access to the Aurora database and DynamoDB.

Answer: C

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/ecs-iam-task-roles-config-errors/>

Question #191

A developer has written an AWS Lambda function using Java as the runtime environment. The developer wants to isolate a performance bottleneck in the code.

Which steps should be taken to reveal the bottleneck?

- A. Use the Amazon CloudWatch API to write timestamps to a custom CloudWatch metric. Use the CloudWatch console to analyze the resulting data.
- B. Use the AWS X-Ray API to write trace data into X-Ray from strategic places within the code. Use the Amazon CloudWatch console to analyze the resulting data.

<https://itexamcertified.com>

<https://itexamcertified.com>

C. Use the AWS X-Ray API to write trace data into X-Ray from strategic places within the code. Use the X-Ray console to analyze the resulting data.

D. Use the Amazon CloudWatch API to write timestamps to a custom CloudWatch metric. Use the AWS X-Ray console to analyze the resulting data.

Answer: C

Reference:

<https://docs.aws.amazon.com/xray/latest/devguide/xray-guide.pdf>

Question #192

A developer added a new feature to an application running on an Amazon EC2 instance that uses Amazon SQS. After deployment, the developer noticed a significant increase in Amazon SQS costs. When monitoring the Amazon SQS metrics on Amazon CloudWatch, the developer found that on average one message per minute is posted on this queue.

What can be done to reduce Amazon SQS costs for this application?

- A. Increase the Amazon SQS queue polling timeout.
- B. Scale down the Amazon SQS queue to the appropriate size for low traffic demand.
- C. Configure push delivery via Amazon SNS instead of polling the Amazon SQS queue.
- D. Use an Amazon SQS first-in, first-out (FIFO) queue instead of a standard queue.

Answer: A

Question #193

A developer is using Amazon DynamoDB to store application data. The developer wants to further improve application performance by reducing response times for read and write operations.

Which DynamoDB feature should be used to meet these requirements?

- A. Amazon DynamoDB Streams
- B. Amazon DynamoDB Accelerator
- C. Amazon DynamoDB global tables
- D. Amazon DynamoDB transactions

Answer: B

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

Question #194

A developer is creating a script to automate the deployment process for a serverless application. The developer wants to use an existing AWS Serverless

Application Model (AWS SAM) template for the application.

What should the developer use for the project? (Choose two.)

- A. Call aws cloudformation package to create the deployment package. Call aws cloudformation deploy to deploy the package afterward.
- B. Call sam package to create the deployment package. Call sam deploy to deploy the package afterward.
- C. Call aws s3 cp to upload the AWS SAM template to Amazon S3. Call aws lambda update-function-code to create the application.
- D. Create a ZIP package locally and call aws serverlessrepo create-application to create the application.
- E. Create a ZIP package and upload it to Amazon S3. Call aws cloudformation create-stack to create the application.

Answer: AB

Reference:

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-getting-started-hello-world.html> <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-cli-package.html>

Question #195

A development team is designing a mobile app that requires multi-factor authentication.

Which steps should be taken to achieve this? (Choose two.)

- A. Use Amazon Cognito to create a user pool and create users in the user pool.
- B. Send multi-factor authentication text codes to users with the Amazon SNS Publish API call in the app code.
- C. Enable multi-factor authentication for the Amazon Cognito user pool.
- D. Use AWS IAM to create IAM users.
- E. Enable multi-factor authentication for the users created in AWS IAM.

Answer: AC

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

<https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-mfa.html#:~:text=To%20configure%20MFA%20in%20the,the%20risk%2Dbased%20adaptive%20authentication.>

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

Question #196

A developer is using AWS CodeDeploy to deploy an application running on Amazon EC2. The developer wants to change the file permissions for a specific deployment file.

Which lifecycle event should a developer use to meet this requirement?

- A. AfterInstall
- B. DownloadBundle
- C. BeforeInstall
- D. ValidateService

Answer: C

You can use the AfterInstall deployment lifecycle event for tasks such as configuring your application or changing file permissions.

Reference:

<https://aws.amazon.com/codedeploy/faqs/>

Question #197

A company is developing a report executed by AWS Step Functions. Amazon CloudWatch shows errors in the Step Functions task state machine. To troubleshoot each task, the state input needs to be included along with the error message in the state output.

Which coding practice can preserve both the original input and the error for the state?

- A. Use ResultPath in a Catch statement to include the error with the original input.
- B. Use InputPath in a Catch statement and set the value to null.
- C. Use Error Equals in a Retry statement to include the error with the original input.
- D. Use OutputPath in a Retry statement and set the value to \$.

Answer: A

Use ResultPath in a Catch to include the error with the original input.

<https://itexamcertified.com>

<https://itexamcertified.com>

Reference:

<https://docs.aws.amazon.com/step-functions/latest/dg/input-output-resultpath.html>

Question #198

A developer is updating an application deployed on AWS Elastic Beanstalk. The new version is incompatible with the old version. To successfully deploy the update, a full cutover to the new, updated version must be performed on all instances at one time, with the ability to roll back changes in case of a deployment failure in the new version.

How can this be performed with the LEAST amount of downtime?

- A. Use the Elastic Beanstalk All at once deployment policy to update all instances simultaneously.
- B. Perform an Elastic Beanstalk Rolling with additional batch deployment.
- C. Deploy the new version in a new Elastic Beanstalk environment and swap environment URLs.
- D. Perform an Elastic Beanstalk Rolling deployment.

Answer: C

Elastic Beanstalk has rolled out a couple of features over the last year that make zero-downtime deployment.

Reference:

<https://rollout.io/blog/batch-deployment-in-aws-elastic-beanstalk/>

Question #199

A developer is writing a web application that must share secure documents with end users. The documents are stored in a private Amazon S3 bucket. The application must allow only authenticated users to download specific documents when requested, and only for a duration of 15 minutes.

How can the developer meet these requirements?

- A. Copy the documents to a separate S3 bucket that has a lifecycle policy for deletion after 15 minutes.
- B. Create a presigned S3 URL using the AWS SDK with an expiration time of 15 minutes.
- C. Use server-side encryption with AWS KMS managed keys (SSE-KMS) and download the documents using HTTPS.
- D. Modify the S3 bucket policy to only allow specific users to download the documents. Revert the change after 15 minutes.

Answer: B

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/>

<https://itexamcertified.com>

Question #200

A developer wants to send multi-value headers to an AWS Lambda function that is registered as a target with an Application Load Balancer (ALB).

What should the developer do to achieve this?

- A. Place the Lambda function and target group in the same account.
- B. Send the request body to the Lambda function with a size less than 1 MB.
- C. Include the Base64 encoding status, status code, status description, and headers in the Lambda function.
- D. Enable the multi-value headers on the ALB.

Answer: D

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/lambda-functions.html#enable-multi-value-headers>

Question #201

An ecommerce startup is preparing for an annual sales event. As the traffic to the company's application increases, the development team wants to be notified when the Amazon EC2 instance's CPU utilization exceeds 80%.

Which solution will meet this requirement?

- A. Create a custom Amazon CloudWatch alarm that sends a notification to an Amazon SNS topic when the CPU utilization exceeds 80%.
- B. Create a custom AWS Cloud Trail alarm that sends a notification to an Amazon SNS topic when the CPU utilization exceeds 80%.
- C. Create a cron job on the EC2 instance that executes the --describe-instance-information command on the host instance every 15 minutes and sends the results to an Amazon SNS topic.
- D. Create an AWS Lambda function that queries the AWS CloudTrail logs for the CPUUtilization metric every 15 minutes and sends a notification to an Amazon SNS topic when the CPU utilization exceeds 80%.

Answer: A

Question #202

An application running on Amazon EC2 opens connections to an Amazon RDS SQL Server database. The developer does not want to store the user name and password for the database in the code. The developer would also like to automatically rotate the credentials.

<https://itexamcertified.com>

What is the MOST secure way to store and access the database credentials?

- A. Create an IAM role that has permissions to access the database. Attach the role to the EC2 instance.
- B. Use AWS Secrets Manager to store the credentials. Retrieve the credentials from Secrets Manager as needed.
- C. Store the credentials in an encrypted text file in an Amazon S3 bucket. Configure the EC2 instance's user data to download the credentials from Amazon S3 as the instance boots.
- D. Store the user name and password credentials directly in the source code. No further action is needed because the source code is stored in a private repository.

Answer: B

Reference:

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>

Question #203

A global company has an application running on Amazon EC2 instances that serves image files from Amazon S3. User requests from the browser are causing high traffic, which results in degraded performance.

Which optimization solution should a developer implement to increase application performance?

- A. Create multiple prefixes in the S3 bucket to increase the request rate.
- B. Create an Amazon ElastiCache cluster to cache and serve frequently accessed items.
- C. Use Amazon CloudFront to serve the content of images stored in Amazon S3.
- D. Submit a ticket to AWS Support to request a rate limit increase for the S3 bucket.

Answer: C

Question #204

An application needs to encrypt data that is written to Amazon S3 where the keys are managed in an on-premises data center, and the encryption is handled by

S3.

Which type of encryption should be used?

- A. Use server-side encryption with Amazon S3-managed keys
- B. Use server-side encryption with AWS KMS-managed keys
- C. Use client-side encryption with customer master key

<https://itexamcertified.com>

<https://itexamcertified.com>

- D. Use server-side encryption with customer-provided keys

Answer: D

Reference:

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

Question #205

A development team is working on a mobile app that allows users to upload pictures to Amazon S3. The team expects the app will be used by hundreds of thousands of users during a single event simultaneously. Once the pictures are uploaded, the backend service will scan and parse the pictures for inappropriate content.

Which approach is the MOST resilient way to achieve this goal, which also smooths out temporary volume spikes for the backend service?

- A. Develop an AWS Lambda function to check the upload folder in the S3 bucket. If new uploaded pictures are detected, the Lambda function will scan and parse them.
- B. Once a picture is uploaded to Amazon S3, publish the event to an Amazon SQS queue. Use the queue as an event source to trigger an AWS Lambda function. In the Lambda function, scan and parse the picture.
- C. When the user uploads a picture, invoke an API hosted in Amazon API Gateway. The API will invoke an AWS Lambda function to scan and parse the picture.
- D. Create a state machine in AWS Step Functions to check the upload folder in the S3 bucket. If a new picture is detected, invoke an AWS Lambda function to scan and parse.

Answer: B

Question #206

A development team wants to run their container workloads on Amazon ECS. Each application container needs to share data with another container to collect logs and metrics.

What should the developer team do to meet these requirements?

- A. Create two pod specifications. Make one to include the application container and the other to include the other container. Link the two pods together.
- B. Create two task definitions. Make one to include the application container and the other to include the other container. Mount a shared volume between the two tasks.
- C. Create one task definition. Specify both containers in the definition. Mount a shared volume between those two containers.
- D. Create a single pod specification. Include both containers in the specification. Mount a persistent volume to both containers.

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: C

Question #207

A company has 25,000 employees and is growing. The company is creating an application that will be accessible to its employees only. A developer is using

Amazon S3 to store images and Amazon RDS to store application data. The company requires that all employee information remain in the legacy Security Assertion Markup Language (SAML) employee directory only and is not interested in mirroring any employee information on AWS.

How can the developer provide authorized access for the employees who will be using this application so each employee can access their own application data only?

- A. Use Amazon VPC and keep all resources inside the VPC, and use a VPC link for the S3 bucket with the bucket policy.
- B. Use Amazon Cognito user pools, federate with the SAML provider, and use user pool groups with an IAM policy.
- C. Use an Amazon Cognito identity pool, federate with the SAML provider, and use an IAM condition key with a value for the cognito-identity.amazonaws.com:sub variable to grant access to the employees.
- D. Create a unique IAM role for each employee and have each employee assume the role to access the application so they can access their personal data only.

Answer: C

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_iam-condition-keys.html

Question #208

A company has developed a new serverless application using AWS Lambda functions that will be deployed using the AWS Serverless Application Model (AWS SAM) CLI.

Which step should the developer complete prior to deploying the application?

- A. Compress the application to a .zip file and upload it into AWS Lambda
- B. Test the new AWS Lambda function by first tracing it in AWS X-Ray
- C. Bundle the serverless application using a SAM package
- D. Create the application environment using the eb create my-env command

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: C

Reference:

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-application-model.pdf>

Question #209

A company stores all personally identifiable information (PII) in an Amazon DynamoDB table named PII in Account A. An application running on Amazon EC2 instances in Account B requires access to the PII table. An administrator in Account A created an IAM role named AccessPII with privileges to access the PII table, and made Account B a trusted entity.

Which combination of additional steps should developers take to access the table? (Choose two.)

- A. Ask an administrator in Account B to allow the EC2 IAM role permission to assume the AccessPII role.
- B. Ask an administrator in Account B to allow the EC2 IAM role permission to assume the AccessPII role with predefined service control policies.
- C. Ask an administrator in Account A to allow the EC2 IAM role permission to assume the AccessPII role with predefined service control policies.
- D. Include the AssumeRole API in the application code logic to obtain credentials to access the PII table.
- E. Include the GetSessionToken API in the application code logic to obtain credentials to access the PII table.

Answer: BD

Question #210

A developer is creating an AWS Lambda function that generates a new file each time it runs. Each new file must be checked into an AWS CodeCommit repository hosted in the same AWS account.

How should the developer accomplish this?

- A. When the Lambda function starts, use the Git CLI to clone the repository. Check the new file into the cloned repository and push the change.
- B. After the new file is created in Lambda, use cURL to invoke the CodeCommit API. Send the file to the repository.
- C. Use an AWS SDK to instantiate a CodeCommit client. Invoke the put_file method to add the file to the repository.
- D. Upload the new to an Amazon S3 bucket. Create an AWS Step Function to accept S3 events. In the Step Function, add the new file to the repository.

Answer: C

<https://itexamcertified.com>

Question #211

A developer must ensure that the IAM credentials used by an application in Amazon EC2 are not misused or compromised.

What should the developer use to keep user credentials secure?

- A. Environment variables
- B. AWS credentials file
- C. Instance profile credentials
- D. Command line options

Answer: C

Question #212

A company has an application where reading objects from Amazon S3 is based on the type of user. The user types are registered user and guest user. The company has 25,000 users and is growing. Information is pulled from an S3 bucket depending on the user type.

Which approaches are recommended to provide access to both user types? (Choose two.)

- A. Provide a different access key and secret access key in the application code for registered users and guest users to provide read access to the objects.
- B. Use S3 bucket policies to restrict read access to specific IAM users.
- C. Use Amazon Cognito to provide access using authenticated and unauthenticated roles.
- D. Create a new IAM user for each user and grant read access.
- E. Use the AWS IAM service and let the application assume the different roles using the AWS Security Token Service (AWS STS) AssumeRole action depending on the type of user and provide read access to Amazon S3 using the assumed role.

Answer: CE

Question #213

A developer is testing an application that invokes an AWS Lambda function asynchronously. During the testing phase, the Lambda function fails to process after two retries.

How can the developer troubleshoot the failure?

- A. Configure AWS CloudTrail logging to investigate the invocation failures

<https://itexamcertified.com>

- B. Configure Dead Letter Queues by sending events to Amazon SQS for investigation
- C. Configure Amazon Simple Workflow Service to process any direct unprocessed events
- D. Configure AWS Config to process any direct unprocessed events

Answer: B

Reference:

<https://www.concurrencylabs.com/blog/how-to-operate-aws-lambda/>

Question #214

A developer is setting up Amazon API Gateway for their company's products. The API will be used by registered developers to query and update their environments. The company wants to limit the amount of requests end users can send for both cost and security reasons. Management wants to offer registered developers the option of buying larger packages that allow for more requests.

How can the developer accomplish this with the LEAST amount of overhead management?

- A. Enable throttling for the API Gateway stage. Set a value for both the rate and burst capacity. If a registered user chooses a larger package, create a stage for them, adjust the values, and share the new URL with them.
- B. Set up Amazon CloudWatch API logging in API Gateway. Create a filter based on the user and requestTime fields and create an alarm on this filter. Write an AWS Lambda function to analyze the values and requester information, and respond accordingly. Set up the function as the target for the alarm. If a registered user chooses a larger package, update the Lambda code with the values.
- C. Enable Amazon CloudWatch metrics for the API Gateway stage. Set up CloudWatch alarms based off the Count metric and the ApiName, Method, Resource, and Stage dimensions to alerts when request rates pass the threshold. Set the alarm action to Deny. If a registered user chooses a larger package, create a user-specific alarm and adjust the values.
- D. Set up a default usage plan, specify values for the rate and burst capacity, and associate it with a stage. If a registered user chooses a larger package, create a custom plan with the appropriate values and associate the plan with the user.

Answer: D

Question #215

A developer is refactoring a monolithic application. The application takes a POST request and performs several operations. Some of the operations are in parallel while others run sequentially. These operations have been refactored into individual AWS Lambda functions. The POST request will be processed by Amazon API

Gateway.

How should the developer invoke the Lambda functions in the same sequence using API Gateway?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Use Amazon SQS to invoke the Lambda functions
- B. Use an AWS Step Functions activity to run the Lambda functions
- C. Use Amazon SNS to trigger the Lambda functions
- D. Use an AWS Step Functions state machine to orchestrate the Lambda functions

Answer: D

Reference:

<https://aws.amazon.com/step-functions/>

Question #216

A company is adding stored value (or gift card) capability to its highly popular casual gaming website. Users need to be able to trade this value for other users' items on the platform. This would require both users' records be updated as a single transaction, or both users' records to be completely rolled back.

Which AWS database options can provide the transactional capability required for this new feature? (Choose two.)

- A. Amazon DynamoDB with operations made with the ConsistentRead parameter set to true
- B. Amazon ElastiCache for Memcached with operations made within a transaction block
- C. Amazon Aurora MySQL with operations made within a transaction block
- D. Amazon DynamoDB with reads and writes made using Transact* operations
- E. Amazon Redshift with operations made within a transaction block.

Answer: CD

Question #217

A developer has created a REST API using Amazon API Gateway. The developer wants to log who and how each caller accesses the API. The developer also wants to control how long the logs are kept.

What should the developer do to meet these requirements?

- A. Enable API Gateway execution logging. Delete old logs using API Gateway retention settings.
- B. Enable API Gateway access logs. Use Amazon CloudWatch retention settings to delete old logs.
- C. Enable detailed Amazon CloudWatch metrics. Delete old logs with a recurring AWS Lambda function.
- D. Create and use API Gateway usage plans. Delete old logs with a recurring AWS Lambda function.

Answer: B

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #218

A company is developing a new web application in Python. A developer must deploy the application using AWS Elastic Beanstalk from the AWS Management Console. The developer creates an Elastic Beanstalk source bundle to upload using the console.

Which of the following are requirements when creating the source bundle? (Choose two.)

- A. The source bundle must include the ebextensions.yaml file
- B. The source bundle must not include a top-level directory
- C. The source bundle must be compressed with any required dependencies in a top-level parent folder
- D. The source bundle must be created as a single .zip or .war file
- E. The source bundle must be uploaded into Amazon EFS

Answer: CD

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/applications-sourcebundle.html>

Question #219

A developer is creating a role to access Amazon S3 buckets. To create the role, the developer uses the AWS CLI create-role command.

Which policy should be added to allow the Amazon EC2 service to assume the role?

- A. Managed policy
- B. Trust policy
- C. Inline policy
- D. Service control policy (SCP)

Answer: B

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html#roles-creatingrole-service-cli

Question #220

<https://itexamcertified.com>

<https://itexamcertified.com>

A company is running a custom application on a set of on-premises Linux servers that are accessed using Amazon API Gateway AWS X-Ray tracing has been enabled on the API test stage.

How can a developer enable X-Ray tracing on the on-premises servers with the LEAST amount of configuration?

- A. Install and run the X-Ray SDK on the on-premises servers to capture and relay the data to the X-Ray service.
- B. Install and run the X-Ray daemon on the on-premises servers to capture and relay the data to the X-Ray service.
- C. Capture incoming requests on-premises and configure an AWS Lambda function to pull, process, and relay relevant data to X-Ray using the PutTraceSegments API call.
- D. Capture incoming requests on-premises and configure an AWS Lambda function to pull, process, and relay relevant data to X-Ray using the PutTelemetryRecords API call.

Answer: B

Question #221

A developer works in an environment with multiple AWS accounts that have AWS Lambda functions processing the same 100 KB payloads. The developer wants to centralize the point of origin of the payloads to one account and have all the Lambda functions be invoked whenever the initiating event occurs in the parent account.

How can the developer design the workflow in the MOST efficient way, so all the multi-account Lambda functions get invoked when the event occurs?

- A. Create a Lambda function in the parent account and use cross-account IAM roles with the AWS Security Token Service (AWS STS) AssumeRole API call to make AWS Lambda invoke the API call to invoke all the cross-account Lambda functions.
- B. Subscribe all the multi-account Lambda functions to an Amazon SNS topic and make a SNS Publish API call with the payload to the SNS topic.
- C. Set up an Amazon SQS queue with the queue policy permitting the ReceiveMessage action for multi-account Lambda functions. Then send the payload to the SQS queue using the sqs:SendMessage permission and poll the queue using multi-account Lambda functions.
- D. Use a worker on an Amazon EC2 instance to poll for the payload event. Invoke all Lambda functions using the Lambda Invoke API after using cross-account IAM roles with the AWS Security Token Service (AWS STS) AssumeRole API call.

Answer: B

Question #222

A large company has its application components distributed across multiple AWS accounts. The company needs to collect and visualize trace data across these accounts.

What should be used to meet these requirements?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. AWS X-Ray
- B. Amazon CloudWatch
- C. Amazon VPC flow logs
- D. Amazon Elasticsearch Service

Answer: A

Reference:

<https://aws.amazon.com/xray/>

Question #223

A startup's photo-sharing site is deployed in a VPC. An ELB distributes web traffic across two subnets. ELB session stickiness is configured to use the AWS-generated session cookie, with a session TTL of 5 minutes.

The webserver Auto Scaling Group is configured as: min-size=4, max-size=4.

The startup is preparing for a public launch, by running load-testing software installed on a single EC2 instance running in us-west-2.

After 60 minutes of load-testing, the webserver logs show:

WEBSERVER LOGS	# of HTTP requests from load-tester	# of HTTP requests from private beta users
webserver #1 (subnet in us-west-2a):	19,210	434
webserver #2 (subnet in us-west-2a):	21,790	490
webserver #3 (subnet in us-west-2b):	0	410
webserver #4 (subnet in us-west-2b):	0	428

Which recommendations can help ensure load-testing HTTP requests are evenly distributed across the four web servers? (Choose two.)

- A. Launch and run the load-tester EC2 instance from us-east-1 instead.
- B. Re-configure the load-testing software to re-resolve DNS for each web request.
- C. Use a 3rd-party load-testing service which offers globally-distributed test clients.
- D. Configure ELB and Auto Scaling to distribute across us-west-2a and us-west-2c.
- E. Configure ELB session stickiness to use the app-specific session cookie.

Answer: BE

<https://itexamcertified.com>

Question #224

A startup's photo-sharing site is deployed in a VPC. An ELB distributes web traffic across two subnets. ELB session stickiness is configured to use the AWS-generated session cookie, with a session TTL of 5 minutes. The webserver Auto Scaling Group is configured as: min-size=4, max-size=4.

The startup is preparing for a public launch, by running load-testing software installed on a single EC2 instance running in us-west-2.

After 60 minutes of load-testing, the webserver logs show:

WEBSERVER LOGS	# of HTTP requests from load-tester	# of HTTP requests from private beta users
webserver #1 (subnet in us-west-2a):	19,210	434
webserver #2 (subnet in us-west-2a):	21,790	490
webserver #3 (subnet in us-west-2b):	0	410
webserver #4 (subnet in us-west-2b):	0	428

Which recommendations can help ensure load-testing HTTP requests are evenly distributed across the four web servers? (Choose two.)

- A. Launch and run the load-tester EC2 instance from us-east-1 instead.
- B. Re-configure the load-testing software to re-resolve DNS for each web request.
- C. Use a 3rd-party load-testing service which offers globally-distributed test clients.
- D. Configure ELB and Auto Scaling to distribute across us-west-2a and us-west-2c.
- E. Configure ELB session stickiness to use the app-specific session cookie.

Answer: BE

Question #225

A development team uses AWS Elastic Beanstalk to deploy a Java-based web application. The team wants to ensure that the changes to the source code and the configuration are always deployed on new instances. The team configures the Elastic Beanstalk environment to use immutable updates. However, an error occurs the first time a change is deployed with the new update policy.

What is the MOST likely cause of this issue?

- A. Immutable updates are not supported for Java-based applications.
- B. The account has reached its on-demand instance limit.
- C. Immutable updates are only supported for m4.large and larger instance types.
- D. The developer must also modify the .ebextensions/immutable-updates.config file to enable immutable updates.

<https://itexamcertified.com>

Answer: D

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environmentmgmt-updates-immutable.html>

Question #226

A developer tested an application locally and then deployed it to AWS Lambda. While testing the application remotely, the Lambda function fails with an access denied message.

How can this issue be addressed?

- A. Update the Lambda function's execution role to include the missing permissions.
- B. Update the Lambda function's resource policy to include the missing permissions.
- C. Include an IAM policy document at the root of the deployment package and redeploy the Lambda function.
- D. Redeploy the Lambda function using an account with access to the AdministratorAccess policy.

Answer: A

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/access-denied-lambda-s3-bucket/>

Question #227

An application contains two components: one component to handle HTTP requests, and another component to handle background processing tasks. Each component must scale independently. The developer wants to deploy this application using AWS Elastic Beanstalk.

How should this application be deployed, based on these requirements?

- A. Deploy the application in a single Elastic Beanstalk environment.
- B. Deploy each component in a separate Elastic Beanstalk environment.
- C. Use multiple Elastic Beanstalk environments for the HTTP component, but one environment for the background task component.
- D. Use multiple Elastic Beanstalk environments for the background task component, but one environment for the HTTP component.

Answer: D

Question #228

<https://itexamcertified.com>

<https://itexamcertified.com>

A company experienced partial downtime during the last deployment of a new application. AWS Elastic Beanstalk split the environment's Amazon EC2 instances into batches and deployed a new version one batch at a time after taking them out of service. Therefore, full capacity was not maintained during deployment.

The developer plans to release a new version of the application, and is looking for a policy that will maintain full capacity and minimize the impact of the failed deployment.

Which deployment policy should the developer use?

- A. Immutable
- B. All at Once
- C. Rolling
- D. Rolling with an Additional Batch

Answer: A

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rolling-version-deploy.html>

Question #229

An application running on multiple Amazon EC2 instances pulls messages from a standard Amazon SQS queue. A requirement for the application is that all messages must be encrypted at rest.

Developers are instructed to use methods that allow for centralized key management and minimize possible support requirements whenever possible.

Which of the following solutions supports these requirements?

- A. Encrypt individual messages by using client-side encryption with customer managed keys, then write to the SQS queue.
- B. Encrypt individual messages by using SQS Extended Client and the Amazon S3 encryption client.
- C. Create an SQS queue, and encrypt the queue by using server-side encryption with AWS KMS.
- D. Create an SQS queue, and encrypt the queue by using client-side encryption.

Answer: B

Question #230

A company is developing a serverless ecommerce web application. The application needs to make coordinated, all-or-nothing changes to multiple items in the company's inventory table in Amazon DynamoDB.

Which solution will meet these requirements?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Enable transactions for the DynamoDB table. Use the BatchWriteItem operation to update the items.
- B. Use the TransactWriteItems operation to group the changes. Update the items in the table.
- C. Set up a FIFO queue using Amazon SQS. Group the changes in the queue. Update the table based on the grouped changes.
- D. Create a transaction table in an Amazon Aurora DB cluster to manage the transactions. Write a backend process to sync the Aurora DB table and the DynamoDB table.

Answer: B

Reference:

<https://aws.amazon.com/blogs/mobile/appsync-caching-transactions/>

Question #231

How can a developer use a debugger for AWS Lambda code that is deployed with AWS Serverless Application Model (AWS SAM)?

- A. Download the Lambda code locally and use the AWS CLI to execute it
- B. Use the Lambda console to connect the debugger
- C. Use AWS SAM to invoke a function locally in debug mode
- D. Connect a third-party-compatible integrated development environment (IDE) to the Lambda debugger endpoint

Answer: C

Reference:

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-sam-cli-using-debugging.html>

Question #232

An application takes longer than expected to process an Amazon SQS message.

What should the developer do to the application so that other instances do not pick up the same message?

- A. Make a ReceiveMessage call to get the same message again from the queue
- B. Issue a DeleteMessage call to delete the message from the queue
- C. Use SendMessage to pass the message to the dead letter queue
- D. Send a ChangeMessageVisibility call to extend VisibilityTimeout

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: A

Question #233

A developer is building a WebSocket API using Amazon API Gateway. The payload sent to this API is JSON that includes an action key. This key can have three different values: create, update, and remove. The developer must integrate with different routes based on the value of the action key of the incoming JSON payload.

How can the developer accomplish this task with the LEAST amount of configuration?

- A. Deploy the WebSocket API to three stages for the respective routes: create, update, and remove
- B. Create a new route key and set the name as action
- C. Set the value of the route selection expression to action
- D. Set the value of the route selection expression to \$request.body.action

Answer: D

Question #234

A development team is creating a new application designed to run on AWS. While the test and production environments will run on Amazon EC2 instances, developers will each run their own environment on their laptops.

Which of the following is the simplest and MOST secure way to access AWS services from the local development machines?

- A. Use an IAM role to assume a role and execute API calls using the role.
- B. Create an IAM user to be shared with the entire development team; provide the development team with the access key.
- C. Create an IAM user for each developer on the team; provide each developer with a unique access key.
- D. Set up a federation through an Amazon Cognito user pool.

Answer: C

Question #235

A developer wants to ensure the Amazon EC2 instances in AWS Elastic Beanstalk execute a certain set of commands before the application is ready to use.

Which Elastic Beanstalk feature will allow the developer to accomplish this?

- A. Rolling update
- B. Immutable update

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. User data
- D. .ebextensions

Answer: D

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/customize-containers-ec2.html>

Question #236

A developer is planning to use an Amazon API Gateway and AWS Lambda to provide a REST API. The developer will have three distinct environments to manage: development, test, and production.

How should the application be deployed while minimizing the number of resources to manage?

- A. Create a separate API Gateway and separate Lambda function for each environment in the same Region.
- B. Assign a Region for each environment and deploy API Gateway and Lambda to each Region.
- C. Create one API Gateway with multiple stages with one Lambda function with multiple aliases.
- D. Create one API Gateway and one Lambda function, and use a REST parameter to identify the environment.

Answer: C

Reference:

<https://aws.amazon.com/blogs/compute/using-api-gateway-stage-variables-to-manage-lambda-functions/>

Question #237

A developer is creating an application to process a large number of requests. Requests must be processed in order, and each request should be processed only once.

How should Amazon SQS be deployed to achieve this?

- A. Configure First in First out (FIFO) delivery in a standard Amazon SQS queue to process requests.
- B. Use an SQS FIFO queue to process requests.
- C. Use the SetOrder attribute to ensure sequential request processing.
- D. Convert the standard queue to a FIFO queue by renaming the queue to use the .fifo suffix.

Answer: B

Reference:

<https://itexamcertified.com>

<https://itexamcertified.com>

<https://medium.com/awesome-cloud/aws-difference-between-sqs-standard-and-fifo-first-in-first-out-queues-28d1ea5e153>

Question #238

A gaming application stores scores for players in an Amazon DynamoDB table that has four attributes: user_id, user_name, user_score, and user_rank. The users are allowed to update their names only. A user is authenticated by web identity federation.

Which set of conditions should be added in the policy attached to the role for the dynamodb: PutItem API call?

<https://itexamcertified.com>

<https://itexamcertified.com>

A.

```
“Condition”: {  
    “ForAllValues:StringEquals”: {  
        “dynamodb:LeadingKeys”: [  
            “${www.amazon.com:user_id}”  
        ],  
        “dynamodb:Attributes”: [  
            “user_name”  
        ]  
    }  
}
```

B.

```
“Condition”: {  
    “ForAllValues:StringEquals”: {  
        “dynamodb:LeadingKeys”: [  
            “${www.amazon.com:user_name}”  
        ],  
        “dynamodb:Attributes”: [  
            “user_id”  
        ]  
    }  
}
```

C.

```
“Condition”: {  
    “ForAllValues:StringEquals”: {  
        “dynamodb:LeadingKeys”: [  
            “${www.amazon.com:user_id}”  
        ],  
        “dynamodb:Attributes”: [  
            “user_name”, “user_id”  
        ]  
    }  
}
```

D.

```
“Condition”: {  
    “ForAllValues:StringEquals”: {  
        “dynamodb:LeadingKeys”: [  
            “${www.amazon.com:user_name}”  
        ],  
        “dynamodb:Attributes”: [  
            “user_name”, “user_id”  
        ]  
    }  
}
```

AnswerC

Question #239

<https://itexamcertified.com>

Given the following AWS CloudFormation template:

```
Description: Creates a new Amazon S3 bucket for shared content. Uses a random bucket name to avoid conflicts.
```

```
Resources:
```

```
ContentBucket:  
    Type: AWS::S3::Bucket  
Outputs:
```

```
ContentBucketName:  
    Value: !Ref ContentBucket
```

What is the MOST efficient way to reference the new Amazon S3 bucket from another AWS CloudFormation template?

- A. Add an Export declaration to the Outputs section of the original template and use ImportValue in other templates.
- B. Add Exported: true to the Contentbucket in the original template and use ImportResource in other templates.
- C. Create a custom AWS CloudFormation resource that gets the bucket name from the ContentBucket resource of the first stack.
- D. Use Fn::Include to include the existing template in other templates and use the ContentBucket resource directly.

AnswerC

Question #240

A developer receives the following error message when trying to launch or terminate an Amazon EC2 instance using a boto3 script.

```
boto.exception.BotoServerError: BotoServerError: 503 Service Unavailable  
<?xml version="1.0" encoding="UTF-8"?>  
<Response><Errors><Error><Code>RequestLimitExceeded</Code>  
<Message>Request limit exceeded.</Message></Error></Errors><RequestId>bfddec84-53b3-4701-b728-dceefb696ced</RequestId>  
</Response>
```

What should the developer do to correct this error message?

- A. Assign an IAM role to the EC2 instance to allow necessary API calls on behalf of the client.
- B. Implement an exponential backoff algorithm for optimizing the number of API requests made to Amazon EC2.

<https://itexamcertified.com>

- C. Increase the overall network bandwidth to handle higher API request rates.
- D. Upgrade to the latest AWS CLI version so that boto3 can handle higher request rates.

AnswerB

Reference:

<https://docs.aws.amazon.com/general/latest/gr/api-retries.html>

Question #241

```
{  
    "FailedRecordCount": 1,  
    "Records": [  
        {  
            "SequenceNumber": "21269319989900637946712965403778482371",  
            "ShardId": "shardId-000000000001"  
  
        },  
        {  
            "ErrorCode": "ProvisionedThroughputExceededException",  
            "ErrorMessage": "Rate exceeded for shard shardId-000000000001 in  
                            stream exampleStreamName under account 123456789."  
        },  
        {  
            "SequenceNumber": "21269319989999637946712965403778482985",  
            "ShardId": "shardId-000000000002"  
        }  
    ]  
}
```

Which techniques will help mitigate this exception? (Choose two.)

- A. Implement retries with exponential backoff
- B. Use a PutRecord API instead of PutRecords
- C. Reduce the frequency and/or size of the requests
- D. Use Amazon SNS instead of Kinesis
- E. Reduce the number of KCL consumers

AnswerAC

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #242

A company processes incoming documents from an Amazon S3 bucket. Users upload documents to an S3 bucket using a web user interface. Upon receiving files in S3, an AWS Lambda function is invoked to process the files, but the Lambda function times out intermittently.

If the Lambda function is configured with the default settings, what will happen to the S3 event when there is a timeout exception?

- A. Notification of a failed S3 event is send as an email through Amazon SNS.
- B. The S3 event is sent to the default Dead Letter Queue.
- C. The S3 event is processed until it is successful.
- D. The S3 event is discarded after the event is retried twice.

AnswerA

Question #243

Which of the following are good use cases for how Amazon ElastiCache can help an application? (Choose two.)

- A. Improve the performance of S3 PUT operations.
- B. Improve the latency of deployments performed by AWS CodeDeploy.
- C. Improve latency and throughput for read-heavy application workloads.
- D. Reduce the time required to merge AWS CodeCommit branches.
- E. Improve performance of compute-intensive applications.

AnswerCE

Reference:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/elasticache-use-cases.html>

Question #244

A developer has designed a customer-facing application that is running on an Amazon EC2 instance. The application logs every request made to it. The application usually runs seamlessly, but a spike in traffic generates several logs that cause the disk to fill up and eventually run out of memory. Company policy requires old logs to be centralized for analysis.

<https://itexamcertified.com>

<https://itexamcertified.com>

Which long-term solution should the developer employ to prevent the issue from reoccurring?

- A. Set up log rotation to rotate the file every day. Also set up log rotation to rotate after every 100 MB and compress the file.
- B. Install the Amazon CloudWatch agent on the instance to send the logs to CloudWatch. Delete the logs from the instance once they are sent to CloudWatch.
- C. Enable AWS Auto Scaling on Amazon Elastic Block Store (Amazon EBS) to automatically add volumes to the instance when it reaches a specified threshold.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to pull the logs from the instance. Configure the rule to delete the logs after they have been pulled.

AnswerC

Question #245

A developer is creating a serverless web application and maintains different branches of code. The developer wants to avoid updating the Amazon API Gateway target endpoint each time a new code push is performed.

What solution would allow the developer to perform a code push efficiently, without the need to update the API Gateway?

- A. Associate different AWS Lambda functions to an API Gateway target endpoint.
- B. Create different stages in API Gateway, then associate API Gateway with AWS Lambda.
- C. Create aliases and versions in AWS Lambda.
- D. Tag the AWS Lambda functions with different names.

AnswerC

Question #246

A developer is building an AWS Lambda function that will dynamically generate and send a weekly newsletter to 100,000 users. This newsletter contains both static text and images. The developer needs a fast and highly scalable place to store the images that will be hyperlinked in the newsletter.

Where should the developer store these images?

- A. Use an Amazon DynamoDB table with DynamoDB Streams and read capacity auto scaling enabled.
- B. Use an Amazon S3 bucket and S3 Transfer Acceleration to speed up the image download.

<https://itexamcertified.com>

<https://itexamcertified.com>

- C. Use an Amazon Aurora database with a public DNS endpoint and auto scaling enabled.
- D. Use an Amazon S3 backed Amazon CloudFront distribution with a high Time-to-Live (TTL) to maximize caching.

AnswerA

Question #247

A developer wants to secure sensitive configuration data such as passwords, database strings, and application license codes. Access to this sensitive information must be tracked for future audit purposes.

Where should the sensitive information be stored, adhering to security best practices and operational requirements?

- A. In an encrypted file on the source code bundle; grant the application access with Amazon IAM
- B. In the Amazon EC2 Systems Manager Parameter Store; grant the application access with IAM
- C. On an Amazon EBS encrypted volume; attach the volume to an Amazon EC2 instance to access the data
- D. As an object in an Amazon S3 bucket; grant an Amazon EC2 instance access with an IAM role

AnswerB

Reference:

<https://aws.amazon.com/blogs/security/how-to-enhance-the-security-of-sensitive-customer-data-by-using-amazon-cloudfront-field-level-encryption/>

Question #248

A developer has built an application using Amazon Cognito for authentication and authorization. After a user is successfully logged in to the application, the application creates a user record in an Amazon DynamoDB table.

What is the correct flow to authenticate the user and create a record in the DynamoDB table?

- A. Authenticate and get a token from an Amazon Cognito user pool. Use the token to access DynamoDB.
- B. Authenticate and get a token from an Amazon Cognito identity pool. Use the token to access DynamoDB.
- C. Authenticate and get a token from an Amazon Cognito user pool. Exchange the token for AWS credentials with an Amazon Cognito identity pool. Use the credentials to access DynamoDB.
- D. Authenticate and get a token from an Amazon Cognito identity pool. Exchange the token for AWS credentials with an Amazon Cognito user pool. Use the credentials to access DynamoDB.

<https://itexamcertified.com>

<https://itexamcertified.com>

AnswerD

Question #249

A Developer is trying to make API calls using SDK. The IAM user credentials used by the application require multi-factor authentication for all API calls.

Which method the Developer use to access the multi-factor authentication protected API?

- A. GetFederationToken
- B. GetCallerIdentity
- C. GetSessionToken
- D. DecodeAuthorizationMessage

Question #250

An application is running on a cluster of Amazon EC2 instances. While trying to read objects stored within a single Amazon S3 bucket that are encrypted with server-side encryption with AWS KMS managed keys (SSE-KMS), the application receives the following error:

Which combination of steps should be taken to prevent this failure? (Choose two.)

- A. Contact AWS Support to request an AWS KMS rate limit increase.
- B. Perform error retries with exponential backoff in the application code.
- C. Contact AWS Support to request a S3 rate limit increase.
- D. Import a customer master key (CMK) with a larger key size.
- E. Use more than one customer master key (CMK) to encrypt S3 data.

AnswerCD

Question #251

<https://itexamcertified.com>

<https://itexamcertified.com>

A developer is building an application integrating an Amazon API Gateway with an AWS Lambda function. When calling the API, the developer receives the following error:

Wed Nov 08 01:13:00 UTC 2017 : Method completed with status: 502

What should the developer do to resolve the error?

- A. Change the HTTP endpoint of the API to an HTTPS endpoint
- B. Change the format of the payload sent to the API Gateway
- C. Change the format of the Lambda function response to the API call
- D. Change the authorization header in the API call to access the Lambda function

AnswerC

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/malformed-502-api-gateway/>

Question #252

How does Envelope Encryption work in AWS KMS?

- A. The Customer Master Key is used to encrypt/decrypt a data key. The Plaintext Data Key is used to encrypt customer data.
- B. Two encryption keys are used. The Customer Master Key encrypts customer data. The Data Key is used to re-encrypt the encrypted data.
- C. Two encryption keys are used. The Data Key encrypts customer data. The Customer Master Key is used to re-encrypt the encrypted data.
- D. The Customer Master Key is used to encrypt/decrypt a data key. The Encrypted Data Key is used to encrypt customer data.

AnswerC

Reference:

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

Question #253

<https://itexamcertified.com>

<https://itexamcertified.com>

A developer must build a mobile application that allows users to read and write data from an Amazon DynamoDB table to store user state for each unique user.

The solution needs to limit data access to allow users access only to their own data.

Which solution below is the most secure?

- A. Embed AWS access credentials into the application and create DynamoDB queries that limit user access.
- B. Use Amazon Cognito identity pools to assign unique identifiers and provide user access.
- C. Modify the DynamoDB table to allow public read and writes, then add client-side filtering.
- D. Create a web portal for users to create an account on AWS Directory Service.

AnswerC

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_dynamodb_specific-table.html

Question #254

A developer is building an application on Amazon EC2. The developer encountered an "Access Denied" error on some of the API calls to AWS services while testing. The developer needs to modify permissions that have been already given to the instance.

How can these requirements be met with minimal changes and minimum downtime?

- A. Make a new IAM role with the needed permissions. Stop the instance. Attach the new IAM role to the instance. Start the instance.
- B. Delete the existing IAM role. Attach a new IAM role with the needed permissions.
- C. Stop the instance. Update the attached IAM role adding the needed permissions. Start the instance.
- D. Update the attached IAM role adding the needed permissions.

AnswerB

Question #255

A developer is building an application that will run on Amazon EC2 instances. The application needs to connect to an Amazon DynamoDB table to read and write records. The security team must periodically rotate access keys.

<https://itexamcertified.com>

<https://itexamcertified.com>

Which approach will satisfy these requirements?

- A. Create an IAM role with read and write access to the DynamoDB table. Generate access keys for the user and store the access keys in the application as environment variables.
- B. Create an IAM user with read and write access to the DynamoDB table. Store the user name and password in the application and generate access keys using an AWS SDK.
- C. Create an IAM role, configure read and write access for the DynamoDB table, and attach to the EC2 instances.
- D. Create an IAM user with read and write access to the DynamoDB table. Generate access keys for the user and store the access keys in the application as a credentials file.

AnswerD

Question #256

A video-hosting website has two types of members: those who pay a fee, and those who do not. Each video upload places a message in Amazon SQS. A fleet of

Amazon EC2 instances polls Amazon SQS and processes each video.

The developer needs to ensure that the videos uploaded by the paying members are processed first.

How can the developer meet this requirement?

- A. Create two SQS queues; one for paying members, and one for non-paying members. Poll the paying member queue first and then poll the non-paying member queue.
- B. Use SQS to set priorities on individual items within a single queue; give the paying members' videos the highest priority.
- C. Use SQS to set priorities on individual items within a single queue and use Amazon SNS to encode the videos.
- D. Create two Amazon SNS topics: one for paying members and one for non-paying members. Use SNS topic subscription priorities to differentiate between the two types of members.

AnswerB

Question #257

A developer is monitoring an application running on an Amazon EC2 instance. The application accesses an Amazon DynamoDB table and the developer has configured a custom Amazon CloudWatch metric with data granularity of 1 second. If there are any issues, the developer wants to be notified within 30 seconds using Amazon SNS.

Which CloudWatch mechanism will satisfy this requirement?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Configure a high-resolution CloudWatch alarm.
- B. Set up a custom AWS Lambda CloudWatch log.
- C. Use a Cloud Watch stream.
- D. Change to a default CloudWatch metric.

AnswerA

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/acw-ug.pdf>

(14)

Question #258

A developer is designing a distributed application built using a microservices architecture spanning multiple AWS accounts. The company's operations team wants to analyze and debug application issues from a centralized account.

How can the developer meet these requirements?

- A. Use an Amazon X-Ray agent with role assumption to publish data into the centralized account.
- B. Use Amazon X-Ray and create a new IAM user to publish the access keys into the centralized account.
- C. Use VPC Flow Logs to collect applications logs across different accounts.
- D. Enable AWS CloudTrail to publish the trails in an Amazon S3 bucket in the centralized account.

AnswerA

Reference:

<https://aws.amazon.com/xray/faqs/#:~:text=Yes%2C%20the%20X-Ray%20agent,application%20into%20a%20central%20account>

Question #259

A developer is implementing authentication and authorization for an application. The developer needs to ensure that the user credentials are never exposed.

Which approach should the developer take to meet this requirement?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Store the user credentials in Amazon DynamoDB. Build an AWS Lambda function to validate the credentials and authorize users.
- B. Deploy a custom authentication and authorization API on an Amazon EC2 instance. Store the user credentials in Amazon S3 and encrypt the credentials using Amazon S3 server-side encryption.
- C. Use Amazon Cognito to configure a user pool, and use the Cognito API to authenticate and authorize the user.
- D. Store the user credentials in Amazon RDS. Enable the encryption option for the Amazon RDS DB instances. Build an API using AWS Lambda to validate the credentials and authorize users.

AnswerC

Reference:

<https://aws.amazon.com/blogs/mobile/understanding-amazon-cognito-user-pool-oauth-2-0-grants/>

Question #260

A developer is building a new complex application on AWS. The application consists of multiple microservices hosted on Amazon EC2. The developer wants to determine which microservice adds the most latency while handling a request.

Which method should the developer use to make this determination?

- A. Instrument each microservice request using the AWS X-Ray SDK. Examine the annotations associated with the requests.
- B. Instrument each microservice request using the AWS X-Ray SDK. Examine the subsegments associated with the requests.
- C. Instrument each microservice request using the AWS X-Ray SDK. Examine the Amazon CloudWatch EC2 instance metrics associated with the requests.
- D. Instrument each microservice request using the Amazon CloudWatch SDK. Examine the CloudWatch EC2 instance metrics associated with the requests.

AnswerC

Question #261

<https://itexamcertified.com>

A company has a two-tier application running on an Amazon EC2 server that handles all of its AWS based e-commerce activity. During peak times, the backend servers that process orders are overloaded with requests. This results in some orders failing to process. A developer needs to create a solution that will re-factor the application.

Which steps will allow for more flexibility during peak times, while still remaining cost-effective? (Choose two.)

- A. Increase the backend T2 EC2 instance sizes to x1 to handle the largest possible load throughout the year.
- B. Implement an Amazon SQS queue to decouple the front-end and backend servers.
- C. Use an Amazon SNS queue to decouple the front-end and backend servers.
- D. Migrate the backend servers to on-premises and pull from an Amazon SNS queue.
- E. Modify the backend servers to pull from an Amazon SQS queue.

AnswerB

Question #262

A developer is asked to integrate Amazon CloudWatch into an on-premises application.

How should the application access CloudWatch, according to AWS security best practices?

- A. Configure AWS credentials in the application server with an AWS SDK
- B. Implement and proxy API-calls through an EC2 instance
- C. Store IAM credentials in the source code to enable access
- D. Add the application server SSH-key to AWS

AnswerA

Question #263

A developer is trying to get data from an Amazon DynamoDB table called demoman-table. The developer configured the AWS CLI to use a specific IAM user's credentials and executed the following command:

The command returned errors and no rows were returned.

What is the MOST likely cause of these issues?

- A. The command is incorrect; it should be rewritten to use put-item with a string argument.

<https://itexamcertified.com>

- B. The developer needs to log a ticket with AWS Support to enable access to the demoman-table.
- C. Amazon DynamoDB cannot be accessed from the AWS CLI and needs to be called via the REST API.
- D. The IAM user needs an associated policy with read access to demoman-table.

AnswerD

Question #264

A company's new mobile app uses Amazon API Gateway. As the development team completes a new release of its APIs, a developer must safely and transparently roll out the API change.

What is the SIMPLEST solution for the developer to use for rolling out the new API version to a limited number of users through API Gateway?

- A. Create a new API in API Gateway. Direct a portion of the traffic to the new API using an Amazon Route 53 weighted routing policy.
- B. Validate the new API version and promote it to production during the window of lowest expected utilization.
- C. Implement an Amazon CloudWatch alarm to trigger a rollback if the observed HTTP 500 status code rate exceeds a predetermined threshold.
- D. Use the canary release deployment option in API Gateway. Direct a percentage of the API traffic using the canarySettings setting.

AnswerD

Question #265

A developer must increase read performance from an unencrypted Amazon S3 bucket. The application requires 100,000 read requests each second. Cost- effectiveness is a priority.

What would be the SIMPLEST approach to implement these requirements?

- A. Create 20 or more prefixes in Amazon S3. Place files by prefixes. Read in parallel by prefixes.
- B. Create 20 or more AWS accounts. Create a bucket in each account. Read in parallel by bucket.
- C. Deploy Memcached on Amazon EC2. Cache the files in memory. Retrieve from the Memcached cache.
- D. Copy all files to Amazon DynamoDB. Index the files with S3 metadata. Retrieve from DynamoDB.

AnswerB

<https://itexamcertified.com>

<https://itexamcertified.com>

Question #266

A developer must modify an Alexa skill backed by an AWS Lambda function to access an Amazon DynamoDB table in a second account. A role in the second account has been created with permissions to access the table.

How should the table be accessed?

- A. Modify the Lambda function execution role's permissions to include the new role.
- B. Change the Lambda function execution role to be the new role.
- C. Assume the new role in the Lambda function when accessing the table.
- D. Store the access key and the secret key for the new role and use them when accessing the table.

AnswerA

Reference:

<https://aws.amazon.com/blogs/security/how-to-create-an-aws-iam-policy-to-grant-aws-lambda-access-to-an-amazon-dynamodb-table/>

Question #267

A developer is creating a new application that will be accessed by users through an API created using Amazon API Gateway. The users need to be authenticated by a third-party Security Assertion Markup Language (SAML) identity provider. Once authenticated, users will need access to other AWS services, such as

Amazon S3 and Amazon DynamoDB.

How can these requirements be met?

- A. Use an Amazon Cognito user pool with SAML as the resource server.
- B. Use Amazon Cognito identity pools with a SAML identity provider as one of the authentication providers.
- C. Use the AWS IAM service to provide the sign-up and sign-in functionality.
- D. Use Amazon CloudFront signed URLs to connect with the SAML identity provider.

Answer: A

Question #268

<https://itexamcertified.com>

<https://itexamcertified.com>

An application development team decides to use AWS X-Ray to monitor application code to analyze performance and perform root cause analysis.

What does the team need to do to begin using X-Ray? (Choose two.)

- A. Log instrumentation output into an Amazon SQS queue.
- B. Use a visualization tool to view application traces.
- C. Instrument application code using the AWS SDK.
- D. Install the X-Ray agent on the application servers.
- E. Create an Amazon DynamoDB table to store the trace logs.

Answer: BD

Reference:

<https://aws.amazon.com/blogs/mt/analyze-debug-applications-aws-x-trace-data-grafana/>

Question #269

A developer has code stored in an Amazon S3 bucket. The code must be deployed as an AWS Lambda function across multiple accounts in the same Region as the S3 bucket. The Lambda function will be deployed using an AWS CloudFormation template that is run for each account.

What is the MOST secure approach to allow access to the Lambda code in the S3 bucket?

- A. Grant the CloudFormation execution role S3 list and get permissions. Add a bucket policy to Amazon S3 with the Principal of `AWS` [account numbers]
- B. Grant the CloudFormation execution role S3 get permissions. Add a bucket policy to Amazon S3 with the Principal of `*`
- C. Use a service-based link to grant the Lambda function S3 list and get permissions by explicitly adding the S3 bucket's account number in the resource.
- D. Use a service-based link to grant the Lambda function S3 get permissions and add a Resource of `*` to allow access to the S3 bucket.

Answer: D

Total 477QA : 208+269 2 sets

<https://itexamcertified.com>

1. AWS Certified Solutions Architect Associate / Mock 7

1. Questions : AWS(Amazon Web Service) Certified Solutions Architect Associate

Questions : AWS(Amazon Web Service)



You are a Solutions Architect for a systems integrator. Your client is growing their presence in the AWS(Amazon Web Service) 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?

Options are :

You cannot connect to multiple AZs from a single location

Use redundant VPN connections to two VGW routers in the region, this should give you access to the infrastructure in all AZs

Order multiple AWS(Amazon Web Service) Direct Connect connections that will be connected to multiple AZs

Order a single AWS(Amazon Web Service) Direct Connect connection to connect to the client's VPC. This will provide access to all AZs within the region

Answer : Order a single AWS(Amazon Web Service) Direct Connect connection to connect to the client's VPC. This will provide access to all AZs within the region

Explanation With AWS(Amazon Web Service) Direct Connect you can provision

a low latency, high performance private connection between the client's data



Tools**chercher.tech****Topic X**

within that region. In this case the client has a single VPC so we know their resources are contained 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) VPC connections use the public Internet



<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

**Take Quiz :****Also Read : AWS Certified Developer Associate Practice Test 2021 Set 14**

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



Tools

chercher.tech

Topic X

Options are :

Auto Scaling

Simple Workflow Service (SWF)

Elastic Beanstalk



Explanation AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS(Amazon Web Service) resources and provision them in an orderly and predictable fashion. AWS(Amazon Web Service) 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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/>

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?

Options are :

You cannot control which nodes your instances are placed on



Tools**chercher.tech****Topic X***Use a Spread Placement Group across two AZs**Use a Cluster Placement Group within a single AZ***Answer : Use a Spread Placement Group across two AZs**

~~Explanation A spread placement group is a group of instances that are each~~



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.

References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

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(Amazon Web Service) services would you use?

Options are :



Tools

chercher.tech

Topic X

RDS

Kinesis

RedShift

Answer : DynamoDB



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 References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>



Take Quiz :



23

Also Read : **AWS Solutions Architect Associate Practice Exams SAA-C01 Set**





Options are :

Disk read operations

Network in and out

CPU utilization

Memory usage

Answer : Memory usage

Explanation ul> There is no standard metric for memory usage on EC2 instances. Use the AWS(Amazon Web Service) website link below for a comprehensive list of the metrics that are collected References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ec2-metricscollected.html>

An application you manage uses an 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)



Tools**chercher.tech****Topic X**

Options are :

Cookies can be inserted by the application or by the load balancer when configured

Sticky sessions are enabled at the target group level

ALB supports load balancer-generated cookies only



Answer : Sticky sessions are enabled at the target group level ALB supports load balancer-generated cookies only

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 References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

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(Amazon Web Service) account. The information that is logged must be encrypted. This requirement applies to all AWS(Amazon Web Service) regions in which your company has services running.

How will you implement this request? (choose 2)



Tools**chercher.tech****Topic X**

Enable encryption with a single KMS key

Use CloudWatch to monitor API calls

Create a CloudTrail trail and apply it to all regions

Create a CloudTrail trail in each region in which you have services



and apply it to all regions

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. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudtrail/>



Take Quiz :



3

Also Read : AWS Solutions Architect - Associate SAA-C01 Practice Exams Set





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)

Options are :

Launch an Elastic Load Balancer and attach it to the Auto Scaling Group

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

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

Use RDS database in a Multi-AZ configuration to add high availability

Use Elasticache Memcached for the datastore to gain high availability across AZs

Answer : Launch an Elastic Load Balancer and attach it to the Auto Scaling Group 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



Tools**chercher.tech****Topic X**

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



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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/> <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/> <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

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(Amazon Web Service) 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(Amazon Web Service) cloud or adding permissions to resources in another AD domain.

Options are :

Install a Microsoft Active Directory Domain Controller on AWS(Amazon Web Service) and add it into your existing on-premise domain

Launch a large AWS(Amazon Web Service) Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication

Launch an AWS(Amazon Web Service) Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain



USE A LARGE AWS(Amazon Web Service) SIMPLE AD IN AWS(Amazon Web Service)

Answer : Launch a large AWS(Amazon Web Service) Directory Service AD

Connector to proxy all authentication back to your on-premise AD service for authentication



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(Amazon Web Service) 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(Amazon Web Service) 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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/>

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

How would you recommend the database tier is deployed?

Options are :

Amazon EC2 instances with Microsoft SQL Server and data replication within an AZ



Amazon RDS with Microsoft SQL Server in a Multi-AZ configuration

Amazon RDS with Microsoft SQL Server

Answer : Amazon EC2 instances with Microsoft SQL Server and data replication between two different AZs

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) References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/> <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/> <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>



Take Quiz :



Also Read : **AWS Certified Developer Associate Practice Test 2021 Set 10**





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?

Options are :

AWS Device Farm

Amazon Cognito

Amazon API Gateway

Application Load Balancer

Answer : Amazon API Gateway

Explanation Amazon API Gateway decouples the client application from the back-end application-layer services by providing a single endpoint for API requests. 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.



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



Options are :

Add a rule in each Security Group that is associated with the affected resources that denies traffic from the identified IP addresses

Add a rule to the Network ACL to deny traffic from the identified IP addresses. Ensure all subnets are associated with the Network ACL

Add a rule in the VPC route table that denies access to the VPC from the identified IP addresses

Configure the NAT Gateway to deny traffic from the identified IP addresses

Answer : Add a rule to the Network ACL to deny traffic from the identified IP addresses. Ensure all subnets are associated with the Network ACL

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.

References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>



c4.large EC2 instance.

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

Options are :



Recreate the API using API Gateway and integrate the API with the existing back-end

Create an Auto Scaling group with a maximum of two instances, then use an Application Load Balancer to balance the traffic

Recreate the API using API Gateway and use AWS(Amazon Web Service) Lambda as the service back-end

Answer : Recreate the API using API Gateway and use AWS(Amazon Web Service) Lambda as the service back-end

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(Amazon Web Service) 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

References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>



Take Quiz :



 Tools

chercher.tech

Topic X

 Architect Associate

X

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?

Options are :

Use EC2 instances instead as you can assign different IAM roles on each instance

In the same Task Definition, specify a separate Task Role for the application container

Create a separate Task Definition for the application container that uses a different Task Role

You cannot implement granular permissions with ECS containers

Answer : Create a separate Task Definition for the application container 

Tools**chercher.tech****Topic X**

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



Definitions and Task Roles References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

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)

Options are :

API Gateway uses the AWS(Amazon Web Service) Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns

API Gateway is a network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS(Amazon Web Service)

Throttling can be configured at multiple levels including Global and Service Call

API Gateway is a collection of resources and methods that are integrated with back-end HTTP endpoints, Lambda functions or other AWS(Amazon Web Service) services

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

Answer : Throttling can be configured at multiple levels including Global and

Service Call API Gateway is a collection of resources and methods that are integrated with back-end HTTP endpoints, Lambda functions or other



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(Amazon Web Service) services. API Gateway handles all of the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls.



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(Amazon Web Service) Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/>

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(Amazon Web Service) services support PFS? (choose 2)

Options are :

Elastic Load Balancing

Auto Scaling

EC2

CloudFront

EBS

Answer : Elastic Load Balancing CloudFront



Tools**chercher.tech****Topic X**

EXPIRATION PROTECTION AND ELD 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 References: <https://digitalcloud.training/certification-training/aws->

**Take Quiz :****Also Read : Practice Exams | AWS Certified Developer Associate 2021 Set 9****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)**

Tools

chercher.tech

Topic X

Stateful

Inbound

Stateless

Deny



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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

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)

Options are :

Set up a NAT gateway in a private subnet to allow the Amazon RedShift cluster to access Amazon S3

Create and configure an Amazon S3 VPC endpoint

Create a NAT gateway in a public subnet to allows the Amazon RedShift cluster to access Amazon S3



Tools**chercher.tech****Topic X**

Create a cluster Security Group to allow the Amazon RedShift cluster to access Amazon S3

Answer : Create and configure an Amazon S3 VPC endpoint Enable Amazon RedShift Enhanced VPC routing



an S3 VPC endpoint will allow S3 to be accessed from other AWS(Amazon Web Service) 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(Amazon Web Service) 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 References:

<https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

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)

Options are :

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

With Network ACLs all rules are evaluated until a permit is encountered or continues until



Tools**chercher.tech****Topic X**

With Network ACLs you can only create allow rules

Answer : 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



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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

**Take Quiz :****Also Read : AWS Certified DevOps Engineer Professional Practice Exams Set****1**

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



Options are :

The ASG will launch three additional EC2 instances in AZ2 and keep the six in AZ1

The ASG will not do anything until the next scaling event

The ASG will launch six additional EC2 instances in AZ2

The ASG will try to rebalance by first creating three new instances in AZ2 and then terminating three instances in AZ1

Answer : The ASG will try to rebalance by first creating three new instances in AZ2 and then terminating three instances in AZ1

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 instances 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.

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>



An EC2 status check on an EBS volume is showing as *insufficient-data*. What is the

Tools**chercher.tech****Topic X**

Options are :

The checks have failed on the volume

The volume does not have enough data on it to check properly



Answer : The checks may still be in progress on the volume

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.

References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeVolumeStatus.html



Take Quiz :



Also Read : AWS SOA-COO Certified Sys Ops Administrator Associate Exam

Set 3





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?

Options are :

The ELB will update Route 53 by removing any references to the instance

The ELB will stop sending traffic to the instance that failed the health check

The ELB will terminate the instance that failed the health check

The ELB will instruct Auto Scaling to terminate the instance and launch a replacement

Answer : The ELB will stop sending traffic to the instance that failed the health check

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.

References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>



You run a two-tier application with a web tier that is behind an Internet-facing

Tools**chercher.tech****Topic X****list of public IP addresses.****What are two possible ways you can implement this requirement? (Choose 2)**

Options are :

*traffic**Configure the ELB security group to allow traffic only from the specific list of IPs**Configure the proxy protocol on the web servers and filter traffic based on IP address**Configure the VPC internet gateway to allow incoming traffic from these IP addresses***Answer : 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****Configure the ELB security group to allow traffic only from the specific list of IPs**

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. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>



Tools**chercher.tech****Topic X**

you need to create a design for the EC2 instances that ensures close proximity, low latency and high network throughput.

Which AWS(Amazon Web Service) features will help you to achieve this requirement whilst considering cost? (choose 2)

Use dedicated hosts

Use Provisioned IOPS EBS volumes

Use EC2 instances with Enhanced Networking

Launch I/O Optimized EC2 instances in one private subnet in an AZ

Answer : Use Placement groups Use EC2 instances with Enhanced

Networking

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 References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>



Take Quiz :





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)

Options are :

The application configuration

The container images to use and the repositories in which they are located

The ELB node to be used to scale the task containers

The security group rules to apply

The ports that should be opened on the container instance for your application

Answer : The container images to use and the repositories in which they are located The ports that should be opened on the container instance for your application

Explanation Some of the parameters you can specify in a task definition



Tools**chercher.tech****Topic X**

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 command the container should run when it is started Environment variables that



References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

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?

Options are :

Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

Add EBS volumes to each EC2 instance and configure data replication

Use the Elastic Block Store (EBS) and mount the file system at the block level

Use the Elastic File System (EFS) and mount the file system using NFS v4.1

Answer : Use the Elastic File System (EFS) and mount the file system using NFS v4.1

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



<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>



Options are :

OpsWorks

Simple Workflow Service

Elastic Beanstalk

CloudFormation

Answer : CloudFormation

Explanation AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS(Amazon Web Service) resources and provision them in an orderly and predictable fashion.

CloudFormation can be used to provision a broad range of AWS(Amazon Web Service) 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 References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/>



Take Quiz :



Also Read • [AWS Devops Engineer Professional Certified Practice Exam Set 3](#)



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?

Options are :

Amazon S3, API Gateway, AWS(Amazon Web Service) Lambda, Amazon RDS

Amazon CloudFront, API Gateway, Amazon S3, AWS(Amazon Web Service) Lambda, DynamoDB

API Gateway, Amazon S3, AWS(Amazon Web Service) Lambda, DynamoDB

Amazon CloudFront, API Gateway, Amazon S3, AWS(Amazon Web Service) Lambda, Amazon RDS

Answer : Amazon CloudFront, API Gateway, Amazon S3, AWS(Amazon Web Service) Lambda, DynamoDB



Tools**chercher.tech****Topic X**

locations around the world. This is the lowest latency option for uploading content. API Gateway and AWS(Amazon Web Service) 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. It is not a serverless service so this option can be ruled out. Amazon S3 alone will not



latency, success routing. However, you would then need to manage uploading the data. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/> <https://aws.amazon.com/blogs/aws/amazon-cloudfront-content-uploads-post-put-other-methods/>

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?

Options are :

Use an AWS(Amazon Web Service) Storage Gateway Virtual Tape Library

Use an AWS(Amazon Web Service) Storage Gateway Volume Gateway in stored volume mode

Use an AWS(Amazon Web Service) Storage Gateway Volume Gateway in cached volume mode



Answer : Use an AWS(Amazon Web Service) Storage Gateway Volume**Gateway in cached volume mode**

Explanation The AWS(Amazon Web Service) Storage Gateway service enables

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.

References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

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(Amazon Web Service) service fits these requirements?

Tools**chercher.tech****Topic X***Security Groups**AWS WAF**Route 53**CloudFront*

Explanation AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS(Amazon Web Service) WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS(Amazon Web Service) 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.

References: <https://aws.amazon.com/waf/details/>

**Take Quiz :**

Also Read : Certification : Get AWS(Amazon Web Service) Certified Solutions Architect Set 4



Your company stores important production data on S3 and you have been asked by



Options are :

Copy your objects to an EBS volume

Enable versioning on the bucket

Use lifecycle actions to backup the data into Glacier

You do not need to do anything, by default versioning is enabled

Use Cross Region Replication to replicate the data to an S3 bucket in another AZ

Answer : Enable versioning on the bucket Use lifecycle actions to backup the data into Glacier

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 question 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(Amazon Web Service) Regions. However, there are data egress costs to consider when copying data across regions.



Tools**chercher.tech****Topic X**

Copying data into an EBS volume would not be cost-effective as it is a higher cost than the other solutions References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

should be highly-available and should scale easily.

Which AWS(Amazon Web Service) service can be used for this design?

Options are :

Amazon S3

Amazon EC2 instance store

Amazon EFS

Amazon EBS

Answer : Amazon EFS

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 References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>



A company runs a service on AWS(Amazon Web Service) 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.

X

Options are :

Amazon Glacier with expedited retrievals

Amazon S3 Standard-Infrequent Access

Amazon S3 Standard

Amazon EFS

Answer : Amazon S3 Standard-Infrequent Access

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>



Take Quiz :



Also Read : **AWS Solutions Architect Associate Practice Exams SAA-C01 Set**

4





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?

Options are :

EMR running Apache Spark

Kinesis Firehose with RDS

Kinesis Firehose with RedShift

EMR using Hive

Answer : Kinesis Firehose with RedShift

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

References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>



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?

ELB predefined Security policies

AES 256

Custom security policies

None of the answers are correct

Security groups

Answer : ELB predefined Security policies Custom security policies

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
References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

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(Amazon Web Service) service should the Architect use to achieve this?

Options are :



Tools

AWS Lambda

Amazon SQS

Amazon STS

Answer · Amazon SNS



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 References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/>



Take Quiz :



8

Also Read : AWS DVA-COO Certified Developer Associate Practice Exam Set



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(Amazon Web Service) Direct Connect and public



Options are :

You can substitute your internet connection at your DC with AWS's public Internet through the use of a NAT gateway in your VPC

You can connect to your private VPC subnets over the public VIF

You can connect to your private VPC subnets over the private VIF, and to Public AWS(Amazon Web Service) services over the public VIF

You can connect to AWS(Amazon Web Service) services over the private VIF

Once connected to your VPC through Direct connect you can connect to all AZs within the region

Answer : You can connect to your private VPC subnets over the private VIF, and to Public AWS(Amazon Web Service) services over the public VIF Once connected to your VPC through Direct connect you can connect to all AZs within the region

Explanation Each AWS(Amazon Web Service) 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(Amazon Web Service) region using AWS(Amazon Web Service) 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



Tools**chercher.tech****Topic X**

Internet References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

X

Recommended Reading

- ⌚ [AWS Certified Cloud Practitioner 6 full practice tests Set 5](#)
- ⌚ [Practice Exams | AWS Certified Cloud Practitioner CLF-C01 Set 16](#)
- ⌚ [AWS ANS-C00 Certified Advanced Networking Practical Exam Set 5](#)
- ⌚ [AWS Certified Developer Associate 2020 \[4 Practice Tests\] Set 3](#)
- ⌚ [Practice Questions : AWS\(Amazon Web Service\) Certified Solutions Architect Associate](#)
- ⌚ [AWS Certified Security Specialty SCS-C01 Practice Exam Set 4](#)
- ⌚ [Practice Exams | AWS Certified Cloud Practitioner CLF-C01 Set 11](#)
- ⌚ [AWS Certified Advanced Networking - Specialty Practice Exam Set 5](#)
- ⌚ [AWS DVA-C01 Certified Developer Associate Practice Exam Set 7](#)
- ⌚ [Practice Exams | AWS Certified Developer Associate 2021 Set 6](#)
- ⌚ [AWS Devops Engineer Professional Certified Practice Exam Set 13](#)
- ⌚ [AWS SOA-C00 Certified Sys Ops Administrator Associate Exam Set 3](#)



Tools**chercher.tech****Comment / Suggestion Section****Topic X**

Enter Name

Enter email (Optional for updates)

X

Suggest Us

Point our Mistakes and Post Your Suggestions

Tools**chercher.tech****TopicX** **ezoic**

report this ad



Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

Tools**chercher.tech****Topic X**

[Tools](#)[chercher.tech](#)[Topics](#)

1. AWS Certified Solutions Architect Associate / Mock 8

1. Practical : AWS(Amazon Web Service) Certified Solutions Architect Associate

Practical : AWS(Amazon Web Service) Certified Solutions Architect Associate

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?

Options are :

Amazon DynamoDB

Amazon RDS

Amazon ElastiCache

Amazon RedShift

Answer : Amazon RedShift

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>



Tools**chercher.tech****Topic X**

performance and scalability. The data will be structured and persistent and the DB must support complex queries using SQL and BI tools.

Which AWS(Amazon Web Service) service will you recommend?

Options are :

RedShift

RDS

DynamoDB

ElastiCache

Answer : RedShift

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

References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>



Take Quiz :



Also Read : AWS DVA-C01 Certified Developer Associate Practice Exam Set 5

You are deploying an application on Amazon EC2 that must call AWS(Amazon Web Service) APIs. Which method of securely passing credentials to the application should you use?

Options are :

Store the API credentials on the instance using instance metadata

Store API credentials as an object in Amazon S3

Embed the API credentials into your application files

Assign IAM roles to the EC2 instances

Answer : Assign IAM roles to the EC2 instances

Explanation Always use IAM roles when you can It is an AWS(Amazon Web Service) best practice not to store API credentials within applications, on file systems or on instances (such as in metadata). References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

You work as a System Administrator at Digital Cloud Training and your manager has



Options are :

Create a Launch Configuration from the instance using the CreateLaunchConfiguration action

Create an Elastic Load Balancer and register the EC2 instance to it

Create a CloudFront distribution and configure the Amazon EC2 instance as the origin

Create an Auto Scaling group from the instance using the CreateAutoScalingGroup action

Answer : Create a CloudFront distribution and configure the Amazon EC2 instance as the origin

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 are more instances to distribute the load to References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

Options are :

With AWS(Amazon Web Service) Lambda you only pay for what you use

AWS Lambda scales automatically

With AWS(Amazon Web Service) lambda, the client is responsible for launching and administering the underlying AWS(Amazon Web Service) compute infrastructure

With AWS(Amazon Web Service) Lambda the customer does not have any responsibility for deploying and managing the compute infrastructure

Answer : With AWS(Amazon Web Service) lambda, the client is responsible for launching and administering the underlying AWS(Amazon Web Service) compute infrastructure

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. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>



Take Quiz :



Also Read : **AWS Certified Cloud Practitioner 6 full practice tests Set 5**

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 fulfil these requirements?

Options are :

Create an ASG with 12 instances spread across 4 AZs behind an ELB

Create an ASG with 18 instances spread across 3 AZs behind an ELB

Create an ASG with 9 instances spread across 3 AZs behind an ELB

Create an ASG with 6 instances spread across 3 AZs behind an ELB

Answer : Create an ASG with 9 instances spread across 3 AZs behind an ELB

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. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

You need to provide AWS(Amazon Web Service) 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(Amazon Web Service) services would you use to configure this access? (choose 2)

Options are :

AWS IAM Groups

AWS Directory Service AD Connector

AWS Directory Service Simple AD

AWS IAM Users

AWS IAM Roles

Answer : AWS Directory Service AD Connector AWS IAM Roles

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(Amazon Web Service) services IAM Roles are created and then "assumed" by trusted entities and define a set of permissions for making AWS(Amazon Web Service) 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



<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/>

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)

Options are :

When reading data from Amazon DynamoDB, users can specify whether they want the read to be eventually consistent or strongly consistent

Supports cross-region replication which allows you to replicate across regions

Data is synchronously replicated across 3 regions

There is no default limit of the throughput you can provision

To scale DynamoDB you must increase the instance size

**Answer : When reading data from Amazon DynamoDB, users can specify whether they want the read to be eventually consistent or strongly consistent
Supports cross-region replication which allows you to replicate across regions**

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/>

Tools**chercher.tech****Topic X****Also Read :** [AWS Devops Engineer Professional Certified Practice Exam Set 2](#)

For which of the following workloads should a Solutions Architect consider using Elastic Beanstalk? (choose 2)

Options are :

A management task run occasionally

A long running worker process

A data lake

A web application using Amazon RDS

Caching content for Internet-based delivery

Answer : A long running worker process A web application using Amazon

X

Tools**chercher.tech****Topic X**

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(Amazon Web Service) Systems Manager Automation References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/>
<https://aws.amazon.com/elasticbeanstalk/faqs/>

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)

Options are :

Backup for on-premises Oracle DB

Complex queries and joins

Migration from a Microsoft SQL relational database

Large amounts of dynamic data that require very low latency

Rapid ingestion of clickstream data

Answer : Large amounts of dynamic data that require very low latency Rapid ingestion of clickstream data

Explanation Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability that

Tools

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

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(Amazon Web Service) services would you recommend to the client? (choose 2)

Options are :

DynamoDB for data ingestion

Kinesis Data Streams for data ingestion

Elasticache for analytics

RedShift for the analytics

EMR for analytics

Answer : DynamoDB for data ingestion RedShift for the analytics

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

Tools

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
References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>

**Take Quiz :****Also Read : AWS Certified Security Speciality SCS-C01 Practice Exam Set 3**

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(Amazon Web Service) feature can act as an instance-level firewall to control traffic between your EC2 instances?

Options are :

Route table

Network ACL

AWS WAF

Security Group

Answer : Security Group

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 References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

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



Options are :

Stop the instance and take the snapshot

Take the snapshot while the EBS volume is attached and the instance is running

Un-mount the EBS volume, take the snapshot, then re-mount it again

You can't take a snapshot for a non-root EBS volume

Answer : Un-mount the EBS volume, take the snapshot, then re-mount it again

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 is fully consistent the requirement is that you minimize application downtime. You can take snapshots of any EBS volume. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

A company needs to deploy virtual desktops for its customers in an AWS(Amazon Web Service) VPC and would like to leverage their existing on-premise security

Tools**chercher.tech****Topic X**

Options are :

A VPN connection, VPC NACLs and Security Groups

A VPN connection, and AWS(Amazon Web Service) Directory Services

AWS Directory Service and AWS(Amazon Web Service) IAM

Amazon EC2, and AWS(Amazon Web Service) IAM

Answer : A VPN connection, and AWS(Amazon Web Service) Directory Services



Take Quiz :



Also Read : QA : AWS(Amazon Web Service) Certified Solutions Architect Associate

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)

Options are :

3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c

2 EC2 instances in ap-southeast-2a, 2 EC2 instances in ap-southeast-2b, 2 EC2 instances in ap-southeast-2c

4 EC2 instances in ap-southeast-2a, 2 EC2 instances in ap-southeast-2b, 2 EC2 instances in ap-southeast-2c

6 EC2 instances in ap-southeast-2a, 6 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c

3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, 3 EC2 instances in ap-southeast-2c

Answer : 6 EC2 instances in ap-southeast-2a, 6 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c 3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, 3 EC2 instances in ap-southeast-2c

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/> <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

Tools**chercher.tech****Topic X**

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?

Options are :

Deploy an ElastiCache Redis cluster with cluster mode disabled and multi-AZ with automatic failover

Deploy an ElastiCache Memcached cluster in multi-AZ mode in the same AZs as RDS

Deploy an ElastiCache Memcached cluster in both AZs in which the RDS database is deployed

Deploy an ElastiCache Redis cluster with cluster mode enabled and multi-AZ with automatic failover

Answer : Deploy an ElastiCache Memcached cluster in both AZs in which the RDS database is deployed

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-

Tools**chercher.tech****Topic X**<https://docs.aws.amazon.com/AmazonElastiCache/latest/mgmt/ug>SelectEngine.html>

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)

Options are :

Auto Scaling has to perform rebalancing first, and then terminate the instance

Auto Scaling has to launch a replacement first before it can terminate the unhealthy instance

If connection draining is enabled, Auto Scaling will wait for in-flight connections to complete or timeout

Auto Scaling will send a notification to the administrator

Auto Scaling will terminate the existing instance before launching a replacement instance

Answer : If connection draining is enabled, Auto Scaling will wait for in-flight connections to complete or timeout Auto Scaling will terminate the existing instance before launching a replacement instance

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 References:

<https://digitalcloud.training/certification-training/aws-solutions-architect->





Set 6

 Also Read : [Practice Tests](#) | AWS Certified Developer Associate 2021- NEW

Set 6

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?

Options are :

Attach an Internet Gateway

Create a VPC endpoint

Deploy NAT Instances in a public subnet

Use a NAT Gateway

X

Tools**chercher.tech****Topic X**

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 References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

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?

Options are :

Protocol - UDP, Port Range - 22, Source 100.156.52.12/0

Protocol - UDP, Port Range - 22, Source 100.156.52.12/32

Protocol - TCP, Port Range - 22, Source 100.156.52.12/0

Protocol - TCP, Port Range - 22, Source 100.156.52.12/32

Answer : Protocol - TCP, Port Range - 22, Source 100.156.52.12/32

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. Configuration of security groups is done at the network interface level.

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?

Options are :

Microsoft SQL Server

Amazon Aurora

Oracle

MySQL

Answer : Amazon Aurora

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 References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_Limits.html



Take Quiz :



Also Read : Practice Exams | AWS Certified Developer Associate 2021 Set 2



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?

Options are :

RedShift

Kinesis Data Streams

Kinesis Firehose

EMR

Answer : Kinesis Data Streams

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(Amazon Web Service) services) Kinesis Firehose can allow transformation of data and it then delivers data to supported services



You are creating a design for an internal-only AWS(Amazon Web Service) 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)

Options are :

Store the access keys and secret IDs within the application

Assign an IAM user for each EC2 instance

Use bastion hosts to enforce control and visibility

Disable root API access keys and secret key

Control user access through network ACLs

Answer : Use bastion hosts to enforce control and visibility Disable root API access keys and secret key

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 References:



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?

Options are :

ELB connection draining

ELB session affinity (sticky session)

ELB proxy protocol

ELB Cross zone load balancing

Answer : ELB connection draining

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 References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>



Take Quiz :



Also Read : [Practice Exams | AWS Certified Developer Associate 2021 Set 2](#)



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)

Options are :

Create a Route 53 hosted zone, and set the NS records of the domain to use Route 53 name servers

Host the website on an Amazon EC2 instance, and map a Route 53 Alias record to the public IP address of the EC2 instance

Host the website using AWS(Amazon Web Service) Elastic Beanstalk, and map a Route 53 Alias record to the Beanstalk stack

Serve the website from an Amazon S3 bucket, and map a Route 53 Alias record to the website endpoint

Host the website on an Amazon EC2 instance with ELB and Auto Scaling, and map a Route 53 Alias record to the ELB endpoint

Answer : Create a Route 53 hosted zone, and set the NS records of the domain to use Route 53 name servers Serve the website from an Amazon S3 bucket, and map a Route 53 Alias record to the website endpoint

Tools**chercher.tech****Topic X**

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.

References: <https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html>

You have been asked to design a cloud-native application architecture using AWS(Amazon Web Service) services. What is a typical use case for SQS?

Options are :

Sending emails to clients when a job is completed

Co-ordination of work items between different human and non-human workers

Providing fault tolerance for S3

Decoupling application components to ensure that there is no dependency on the availability of a single component

Answer : Decoupling application components to ensure that there is no dependency on the availability of a single component

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

email notifications when certain events happen References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

A new security mandate requires that all personnel data held in the cloud is encrypted at rest. Which two methods allow you to encrypt data stored in S3 buckets at rest cost-efficiently? (choose 2)

Options are :

Make use of AWS(Amazon Web Service) S3 bucket policies to control access to the data at rest

Use AWS(Amazon Web Service) S3 server-side encryption with Key Management Service keys or Customer-provided keys

Encrypt the data at the source using the client's CMK keys before transferring it to S3

Use CloudHSM

Use Multipart upload with SSL

Answer : Use AWS(Amazon Web Service) S3 server-side encryption with Key Management Service keys or Customer-provided keys Encrypt the data at the source using the client's CMK keys before transferring it to S3

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



Tools**chercher.tech****Topic X**

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 can be used to encrypt data but as a dedicated service it is charged on an hourly basis and is less cost-efficient compared to S3 encryption or encrypting the data at the source. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

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?

Tools

Amazon Redshift

chercher.tech**Topic X***Amazon EFS***Answer : Amazon EFS**

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

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(Amazon Web Service) principals in other accounts within the region to consume. Based on this model, what AWS(Amazon Web Service) service will be used to offer the service for consumption?

Options are :

*API Gateway**VPC Endpoint Services using AWS(Amazon Web Service) PrivateLink**Route 53**IAM Role Based Access Control***Answer : VPC Endpoint Services using AWS(Amazon Web Service)****X**

Tools**chercher.tech****Topic X**

entry point for traffic destined to a supported service Using PrivateLink you can connect your VPC to supported AWS(Amazon Web Service) services, services hosted by other AWS(Amazon Web Service) accounts (VPC endpoint services), and supported AWS(Amazon Web Service) Marketplace partner services References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

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?

Options are :

Security patching

Updating DB parameter groups

Promoting a Read Replica

Selecting the Multi-AZ feature

Answer : Security patching

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 brie

Recommended Reading

 **AWS Develops Engineer Professional Practice Final File Exam Set 9**



1. AWS Certified Solutions Architect Associate / Mock 6**1. Exam : AWS(Amazon Web Service) Certified Solutions Architect Associate**

Exam : AWS(Amazon Web Service) Certified Solutions Architect Associate

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)

Options are :

Use HDD, Cold (SC1) EBS volumes

Use a larger instance size within the instance family

Use Provisioned IOPS (IOP1) EBS volumes

Use EBS optimized instances

Create a RAID 1 array from multiple EBS volumes

Answer : Use Provisioned IOPS (IOP1) EBS volumes Use EBS optimized instances

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



Tools**chercher.tech****Topic X**

performance References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

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)

Options are :

The failover mechanism automatically moves the Elastic IP address of the instance to the standby DB instance

The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance

Failover times are typically 60-120 seconds

Multi-AZ uses synchronous replication; therefore, the failover is instantaneous

Answer : The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance Failover times are typically 60-120 seconds

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 DNS record is updated, not the IP address.



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X**~~associate/database/databases/~~**Take Quiz :****Set 1****Also Read : AWS SOA-COO Certified Sys Ops Administrator Associate Exam**

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?

Options are :

The alarm state will be immediately set to INSUFFICIENT DATA



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools

The ASG will automatically update the frequency of the alarms to 300 seconds to match the EC2 monitoring in the launch configuration

The EC2 metrics will be updated automatically to match the frequency of the alarms and send updates every 60 seconds

Answer : 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

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 References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-monitoring.html#as-group-metrics>

When using the MySQL database with AWS(Amazon Web Service) 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?

Options are :

Acrobat Pro DC
Perfect your resume as a PDF.

Try free

Memory

Answer : InnoDB

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". References:

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

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

One of your clients is transitioning their web presence into the AWS(Amazon Web Service) cloud. As part of the migration the client will be running a web application both on-premises and in AWS(Amazon Web Service) 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?

Options are :

Use an Application Load Balancer to distribute traffic based on IP address

Use Route 53 with a simple routing policy

Use a Network Load Balancer to distribute traffic based on Instance ID

Use Route 53 with a weighted routing policy and configure the respective weights

~~Answer : Use Route 53 with a weighted routing policy and configure the respective weights~~



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X**

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(Amazon Web Service) and on-premise resources using IP addresses (not Instance IDs) Application Load Balancer can distribute traffic to AWS(Amazon Web Service) and on-premise resources using IP addresses but cannot be used to distribute traffic in a weighted manner References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

**Take Quiz :****Set 3****Also Read : Practice Tests | AWS Certified Developer Associate 2021- NEW****Acrobat Pro DC****Perfect your resume as a PDF.****Try free**

Tools**chercher.tech****Topic X**

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(Amazon Web Service) services for these functions. Which services and frameworks should be used for the system monitoring and deployment layers? (choose 2)

Options are :

Use AWS(Amazon Web Service) Lambda to package, test, and deploy the serverless application stack

Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics

Use AWS(Amazon Web Service) X-Ray to package, test, and deploy the serverless application stack

Use AWS(Amazon Web Service) SAM to package, test, and deploy the serverless application stack

Use Amazon CloudTrail for consolidating system and application logs and monitoring custom metrics

Answer : Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics Use AWS(Amazon Web Service) SAM to package, test, and deploy the serverless application stack

Explanation AWS Serverless Application Model (AWS SAM) is an extension of AWS(Amazon Web Service) CloudFormation that is used to package, test, and deploy serverless applications. With Amazon CloudWatch, you can access system metrics on all the AWS(Amazon Web Service) services you use, consolidate system and application level logs, and create business key performance indicators (KPIs) as



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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 References:

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

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/>

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)

Options are :

There are no inbound rules and traffic will be implicitly denied

There is an outbound rule that allows all traffic to all IP addresses

There is an outbound rule allowing traffic to the Internet Gateway

There is an inbound rule that allows traffic from the Internet Gateway

There is an inbound rule allowing traffic from the Internet to port 22 for management

Answer : There are no inbound rules and traffic will be implicitly denied

There is an outbound rule that allows all traffic to all IP addresses

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

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(Amazon Web Service) best practices, what can you do to optimize performance?

Options are :

Integrate CloudFront with S3 to cache the content

Use ElastiCache to cache the content

Use S3 Transfer Acceleration

Use cross-region replication to spread the load across regions

Answer : Integrate CloudFront with S3 to cache the content

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X**<https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html><https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>**Take Quiz :****Also Read : AWS Devops Engineer Professional Certified Practice Exam Set****10**

Your company has started using the AWS(Amazon Web Service) 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?



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Log a case with AWS(Amazon Web Service) support and they will use MFA to recover the credentials

Reset the CloudHSM device and create a new set of credentials

Answer : There is no way to recover your keys if you lose your credentials

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 References:
<https://aws.amazon.com/cloudhsm/faqs/>

You have implemented the AWS(Amazon Web Service) 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)

Options are :

Use Network ACLs to control the traffic

Use EFS Security Groups to control network traffic

Use AWS(Amazon Web Service) Web Application Firewall (WAF) to protect EFS

Use POSIX permissions to control access from hosts by user or group

Use IAM groups to control access by user or group

Answer : Use EFS Security Groups to control network traffic Use POSIX



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X**

by user and group. EFS Security Groups act as a firewall, and the rules you add define the traffic flow. You cannot use AWS(Amazon Web Service) 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. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>
<https://aws.amazon.com/efs/features/>

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?

Options are :

Configure Access Logs to be delivered to S3 and use EMR for processing the log files

Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files

Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files

Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files

Answer : Configure Access Logs to be delivered to S3 and use EMR for processing the log files

Explanation Access Logs can be enabled on ALB and configured to store data

The advertisement features the Adobe logo and the text "Acrobat Pro DC" and "Perfect your resume as a PDF." It includes a "Try free" button and a small image of a resume.

Tools**chercher.tech****Topic X**

access logs to be delivered to DynamoDB References:

[https://digitalcloud.training/certification-training/aws-solutions-architect-](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/)

[associate/analytics/amazon-emr/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/)

**Take Quiz :****Also Read : AWS Devops Engineer Professional Certified Practice Exam Set 11**

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.



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools

chercher.tech

Topic X

EBS General Purpose SSD

EBS Provisioned IOPS SSD

EBS General Purpose SSD in a RAID 1 configuration

EBS Throughput Optimized HDD

Answer : EBS Throughput Optimized HDD

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.

References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

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?

Options are :

Use enhanced networking

Add multiple Elastic IP addresses to the instance

Create a placement group and put the EC2 instance in it



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



[Tools](#)[chercher.tech](#)[Topic X](#)

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). References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

<https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/>

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?



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received

Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once

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

Answer : 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

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

References:



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



[Tools](#)[chercher.tech](#)[Topic X](#)[Take Quiz :](#)[Set 4](#)[Also Read : AWS Certified SysOps Administrator Associate Practice Exams](#)[Set 4](#)

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?

Options are :

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.

[Acrobat Pro DC](#)[Perfect your resume as a PDF.](#)[Try free](#)

Answer : 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

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) References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Options are :

Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class

Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old

Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old

Use an S3 bucket policy that deletes objects that are more than 60 days old

Answer : Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old

Explanation Moving logs to Glacier may save cost but the question 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. References: <https://aws.amazon.com/about-aws/whats-new/2011/12/27/amazon-s3-announces-object-expiration/> <https://aws.amazon.com/about-aws/whats-new/2011/12/27/amazon-s3-announces-object-expiration/>

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Create a DynamoDB Auto Scaling scaling policy

Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput

Create a CloudWatch alarm that triggers an AWS(Amazon Web Service) Lambda function that adjusts the provisioned throughput

Answer : Create a DynamoDB Auto Scaling scaling policy

Explanation DynamoDB auto scaling uses the AWS(Amazon Web Service) 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(Amazon Web Service) 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. References:

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



Take Quiz :



Also Read : AWS BDS-COO Certified Big Data Speciality Practice Test Set 7



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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?

Options are :

Amazon EC2 instances with Microsoft SQL Server and data replication between two different AZs

Amazon EC2 instances with Microsoft SQL Server and data replication within an AZ

Amazon RDS with Microsoft SQL Server

Amazon RDS with Microsoft SQL Server in a Multi-AZ configuration

Answer : Amazon RDS with Microsoft SQL Server in a Multi-AZ configuration

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X**

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/> <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

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(Amazon Web Service) service will securely connect the devices to the cloud applications?

Options are :

AWS DMS

AWS Glue

AWS Lambda

AWS IoT Core

Answer : AWS IoT Core

Explanation 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

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?



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools

chercher.tech

Topic X

On-Demand

Dedicated instances

Spot

Answer : On-Demand

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(Amazon Web Service) 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 References:

<https://aws.amazon.com/ec2/pricing/>



Take Quiz :



Also Read : AWS Devops Engineer Professional Certified Practice Exam Set 7



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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)

Options are :

All instance types support encryption

All attached EBS volumes must share the same encryption state

Data in transit between an instance and an encrypted volume is also encrypted

Not all EBS types support encryption

There is no direct way to change the encryption state of a volume

Answer : Data in transit between an instance and an encrypted volume is also encrypted There is no direct way to change the encryption state of a volume

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

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(Amazon Web Service) must be directed over the VPN to the corporate firewall. How can this be achieved?



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



In the public subnet route table, add a route for your remote network and specify the customer gateway as the target

Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway

In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway

Answer : In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target

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.

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

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech**

Topic X

*Classic Load Balancer**Network Load Balancer**Application Load Balancer**Route 53***Answer : Network Load Balancer**

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).

References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

**Take Quiz :****5****Also Read : AWS Solutions Architect Associate Practice Exams SAA-C01 Set****Acrobat Pro DC****Perfect your resume as a PDF.****Try free**

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)

Options are :

Cross-subnet

Within an Availability Zone

Cross-Continent

Cross-Availability Zone

Cross-Facility

Answer : Within an Availability Zone Cross-Availability Zone

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. References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Options are :

AWS Glue

AWS OpsWorks

AWS CodeDeploy

AWS CodePipeline

AWS Cognito

Answer : AWS CodeDeploy AWS CodePipeline

Explanation You can automate your serverless application's release process using AWS(Amazon Web Service) CodePipeline and AWS(Amazon Web Service) CodeDeploy. The following AWS(Amazon Web Service) 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(Amazon Web Service) CodeDeploy to gradually deploy updates to your serverless applications. You use CodeBuild to build, locally test, and package your serverless application. You use AWS(Amazon Web Service) CloudFormation to deploy your application. References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/> <https://docs.aws.amazon.com/lambda/latest/dg/build-pipeline.html>

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.



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X***Parameters**Metadata**Tags**User data***Answer : Metadata**

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 References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html#instancedata-data-categories>

**Take Quiz :****Set 1****Also Read : AWS SOA-COO Certified Sys Ops Administrator Associate Exam****Acrobat Pro DC****Perfect your resume as a PDF.****Try free**

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(Amazon Web Service) resources and are looking for a service that can handle the provisioning and management of the underlying resources it will run on.

What AWS(Amazon Web Service) service would allow the developers to upload the Java source code file and provide capacity provisioning and infrastructure management?

Options are :

AWS CloudFormation

AWS CodeDeploy

AWS OpsWorks

AWS Elastic Beanstalk

Answer : AWS Elastic Beanstalk

Explanation AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS(Amazon Web Service) 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), and then



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/> <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

A development team are creating a Continuous Integration and Continuous Delivery (CI/CD) toolchain on the AWS(Amazon Web Service) cloud. The team currently use Jenkins X and Kubernetes on-premise and are looking to utilize the same services in the AWS(Amazon Web Service) cloud.

What AWS(Amazon Web Service) service can provide a managed container platform that is MOST similar to their current CI/CD toolchain?

Options are :

AWS CodePipeline

Amazon ECS

AWS Lambda

Amazon EKS

Answer : Amazon EKS

Explanation Amazon EKS is AWS' managed Kubernetes offering, which enables you to focus on building applications, while letting AWS(Amazon Web Service) handle managing Kubernetes and the underlying cloud infrastructure Amazon



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



automate your release pipelines for fast and reliable application and infrastructure updates. It is not a container platform References: <https://aws.amazon.com/eks/>

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?

Options are :

Use CloudFront's DDoS prevention features

Use a Security Group rule that denies connections from the block of IP addresses

Use a Network ACL rule that denies connections from the block of IP addresses

Create a Bastion Host restrict all connections to the Bastion Host only

Answer : Use a Network ACL rule that denies connections from the block of IP addresses

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X**

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 References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

**Take Quiz :**

Also Read : Certification : AWS(Amazon Web Service) Certified Solutions Architect Associate

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.



Acrobat Pro DC



Perfect your resume as a PDF.

Try free



X

Options are :

Amazon Kinesis Data Streams

Amazon S3 Select

Amazon RedShift Spectrum

Amazon Elasticsearch

Amazon SWF

Answer : Amazon S3 Select Amazon RedShift Spectrum

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 References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/> <https://aws.amazon.com/blogs/aws/s3-glacier-select/> <https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-redshift-spectrum-is-now-available-in-four-additional-aws-regions-and-enhances-query-performance-in-all-available-aws-regions/>



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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?

Options are :

Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances

Add more c5.large instances to spread the load more evenly

Add all of the instances into a Placement Group

Change the configuration to use only c4.2xlarge instance types

Answer : Change the configuration to use only c4.2xlarge instance types

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

References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

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)



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



server security group

Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway

Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32

Answer : Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0 Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group

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
References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>



Take Quiz :



Also Read : **AWS DVA-C01 Certified Developer Associate Practice Exam Set 6**



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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?

Options are :

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

You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume

You can specify the instance store volumes for your instance only when you launch an instance

You must shutdown the instance in order to be able to add the instance store volume

Answer : You can specify the instance store volumes for your instance only when you launch an instance

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.



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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)

Options are :

There is a default inbound rule allowing traffic from the VPC CIDR block

There is a default inbound rule denying all traffic

There is a default outbound rule allowing traffic to the Internet Gateway

There is a default outbound rule allowing all traffic

There is a default outbound rule denying all traffic

Answer : There is a default inbound rule denying all traffic There is a default outbound rule denying all traffic

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.

References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech**

Topic X

*Data is replicated globally**Data is resilient in the event of one entire Availability Zone destruction**Data is resilient in the event of one entire region destruction**Provides 99.999999999% durability of archives**Provides 99.9% availability of archives***Answer : Data is resilient in the event of one entire Availability Zone****destruction Provides 99.999999999% durability of archives**

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. References: <https://aws.amazon.com/s3/storage-classes/>

**Take Quiz :****Also Read : AWS DVA-COO Certified Developer Associate Practice Exam Set****10****Acrobat Pro DC****Perfect your resume as a PDF.****Try free**

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?

Options are :

Metadata

AWS Config

User data

Run command

Answer : User data

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(Amazon Web Service) Systems Manager run command is used to manage the configuration of existing instances by using remotely executed commands. User data is better for specifying



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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?

Options are :

This is possible using the Classic Load Balancer (CLB) if using Instance IDs

This is not possible with ELB, you would need to use Route 53

No, the instances that an ELB routes traffic to must be in the same VPC

This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets

Answer : This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets

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(Amazon Web Service) through Direct Connect or a VPN connection References: <https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/> <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

One of the applications you manage receives a high traffic loads between 7:30am and 9:30am daily. The application uses an Auto Scaling Group (ASG) to maintain 3



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Options are :

Use a Dynamic scaling policy

Use a Simple scaling policy

Use a Scheduled scaling policy

Use a Step scaling policy

Answer : Use a Scheduled scaling policy

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

References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>



Take Quiz :



Also Read : **AWS Solutions Architect Associate Practice Exams SAA-C01 Set**

33



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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(Amazon Web Service) service can be used for this requirement?

Options are :

Amazon RedShift

Amazon Kinesis Firehose

Amazon RDS

Amazon Neptune

Answer : Amazon RedShift

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Options are :

Sticky Sessions

Connection Draining

Deletion Protection

Proxy Protocol

Answer : Connection Draining

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

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(Amazon Web Service) service can deliver these requirements?



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X***EC2 instances with EBS replication**RDS with Multi-AZ***Answer : RDS with cross-region Read Replicas**

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

References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

**Take Quiz :****Also Read : AWS Certified Developer Associate Practice Test 2021 Set 2**

Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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(Amazon Web Service) 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(Amazon Web Service) resources (including the AWS(Amazon Web Service) Management Console) using single sign-on (SSO).

What is the simplest way to enable SSO to the AWS(Amazon Web Service) management console using the existing domain?

Options are :

Launch an Enterprise Edition AWS(Amazon Web Service) Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain

Install a Microsoft Active Directory Domain Controller on AWS(Amazon Web Service) and add it into your existing on-premise domain

Launch a large AWS(Amazon Web Service) Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication

Use a large AWS(Amazon Web Service) Simple AD in AWS(Amazon Web Service)

Answer : Launch an Enterprise Edition AWS(Amazon Web Service) Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain

Explanation With the AWS(Amazon Web Service) Active Directory Service for Microsoft Active Directory you can setup trust relationships to extend authentication from on-premises Active Directories into the AWS(Amazon Web Service) cloud. You can also use Active Directory credentials to authenticate to the



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X**

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 References:
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/>

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?

Options are :

Outputs

Resources

Mappings

Parameters

Answer : Outputs

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(Amazon Web Service) 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)



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**chercher.tech****Topic X**

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/outputs-section-structure.html>

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?

Options are :

Use AWS(Amazon Web Service) Import/Export

Use Multipart Upload

Use a single PUT request to upload the large file

Use Amazon Snowball

Answer : Use Multipart Upload

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(Amazon Web Service) and they import your data into S3. It is not used for single files.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>



Take Quiz :



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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?

Options are :

On-demand instances

Reserved instances

Spot instances

Flexible instances

Answer : Reserved instances

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



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



There's no such thing as flexible instances References:

[https://digitalcloud.training/certification-training/aws-solutions-architect-](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/)

[associate/compute/amazon-ec2/ https://aws.amazon.com/ec2/pricing/reserved-instances/](https://aws.amazon.com/ec2/pricing/reserved-instances/)

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)

Options are :

The default DB security group is applied to the new DB instance

The database restore overwrites the existing database

You can restore up to the last 1 minute

Custom DB security groups are applied to the new DB instance

You can restore up to the last 5 minutes

Answer : The default DB security group is applied to the new DB instance You can restore up to the last 5 minutes

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 References:



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



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(Amazon Web Service) terminated the Spot instance. The Spot instance had not finished processing the message. What will happen to the message?

Options are :

The message will become available for processing again after the visibility timeout expires

The message will be lost as it would have been deleted from the queue when processed

The message will remain in the queue and be immediately picked up by another instance

The results may be duplicated in DynamoDB as the message will likely be processed multiple times

Answer : The message will become available for processing again after the visibility timeout expires

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 References:



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



Tools**Take Quiz :****chercher.tech****Topic X****Also Read : Practice Exams | AWS Certified Developer Associate 2021 Set 5**

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?

Options are :

Check that the subnet CIDR block is referenced properly in the route table

Check that the VPN is configured correctly

Check that the Security Groups and Network ACLs have the correct rules configured

Check that there is a Bastion Host in the subnet and connect to it first

**Acrobat Pro DC****Perfect your resume as a PDF.****Try free**

Tools

chercher.tech

Topic X

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 References: <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>
<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

Recommended Reading

⌚ AWS Certified Advanced Networking ⇢ Speciality(ANS-COO) Exam Set 6



Acrobat Pro DC

Perfect your resume as a PDF.

Try free



[101. WEB IDENTITY FEDERATION – COGNITO](#) [102. REDUCING SECURITY THREATS](#)[103. KEY MANAGEMENT SERVICE \(KMS\)](#) [104. CLOUD HSM](#) [105. PARAMETER STORE](#)[106. LAMBDA](#) [107. BUILD A SERVERLESS WEBPAGE WITH API GATEWAY AND LAMBDA](#)[108. BUILD AN ALEXA SKILL](#) [109. SERVERLESS APPLICATION MODEL \(SAM\)](#)[110. ELASTIC CONTAINER SERVICE \(ECS\)](#) [111. MISCELLANEOUS](#)[BIG DATA](#) [DATA SCIENCE](#) [DEVOPS](#) [AZURE](#) [RESUME](#)

AWS Dumps

1. IAM
2. Billing Alarm
3. S3
4. Creation of S3 Bucket
5. S3 Pricing Tiers
6. S3 Security and Encryption
7. S3 Version Control
8. S3 Life Cycle Management
9. S3 Lock Policies and Glacier Vault Lock
10. S3 Performance
11. S3 Select and Glacier Select
12. AWS Organizations & Consolidate Billing
13. Sharing S3 Buckets between Accounts
14. Cross Region Replication
15. Transfer Acceleration
16. DataSync Overview
17. CloudFront Overview
18. CloudFront Signed URL's and Cookies
19. Snowball
20. Storage Gateway
21. Athena versus Macie
22. EC2
23. Security Groups
24. EBS
25. Volumes & Snapshots
26. AMI Types (EBS vs Instance Store)
27. ENI vs ENA vs EFA
28. Encrypted Root Device Volumes & Snapshots
29. Spot Instances & Spot Fleets
30. EC2 Hibernate
31. Cloud Watch
32. AWS Command Line
33. IAM Roles with EC2
34. Boot Strap Scripts
35. EC2 Instance Meta Data
36. EFS
37. FSX for Windows & FSX for Lustre
38. EC2 Placement Groups



- 39. HPC
- 40. WAF
- 41. Databases
- 42. Create an RDS Instance
- 43. RDS Backups, Multi-AZ & Read Replicas
- 44. Dynamo DB
- 45. Advanced Dynamo DB
- 46. Redshift
- 47. Aurora
- 48. ElastiCache
- 49. Database Migration Services (DMS)
- 50. Caching Strategies
- 51. EMR
- 52. Directory Service
- 53. IAM Policies
- 54. Resource Access Manager (RAM)
- 55. Single Sign-On
- 56. Route 53 – Domain Name Server (DNS)
- 57. Route 53 – Register a Domain Name Lab
- 58. Route 53 Routing Policies
- 59. Route 53 Simple Routing Policy
- 60. Route 53 Weighted Routing Policy
- 61. Route 53 Latency Routing Policy
- 62. Route 53 Failover Routing Policy
- 63. Route 53 Geolocation Routing Policy
- 64. Route 53 Geoproximity Routing Policy (Traffic Flow Only)
- 65. Route 53 Multivalue Answer
- 66. VPCs
- 67. Build a Custom VPC
- 68. Network Address Translation (NAT)
- 69. Access Control List (ACL)
- 70. Custom VPCs and ELBs
- 71. VPC Flow Logs
- 72. Bastions
- 73. Direct Connect
- 74. Setting Up a VPN Over a Direct Connect Connection
- 75. Global Accelerator
- 76. VPC End Points
- 77. VPC Private Link
- 78. Transit Gateway
- 79. VPN Hub
- 80. Networking Costs
- 81. ELB
- 82. ELBs and Health Checks – LAB
- 83. Advanced ELB
- 84. ASG
- 85. Launch Configurations & Autoscaling Groups Lab
- 86. HA Architecture
- 87. Building a fault tolerant WordPress site – Lab 1
- 88. Building a fault tolerant WordPress site – Lab 2
- 89. Building a fault tolerant WordPress site – Lab 3 : Adding Resilience & Autoscaling
- 90. Building a fault tolerant WordPress site – Lab 4 : Cleaning Up
- 91. Building a fault tolerant WordPress site – Lab 5 : Cloud Formation



- 92. Elastic Beanstalk Lab
 - 93. Highly Available Bastions
 - 94. On Premise Strategies
 - 95. SQS
 - 96. SWF
 - 97. SNS
 - 98. Elastic Transcoder
 - 99. API Gateway
 - 100. Kinesis
 - 101. Web Identity Federation – Cognito
 - 102. Reducing Security Threats
 - 103. Key Management Service (KMS)
 - 104. Cloud HSM
 - 105. Parameter Store
 - 106. Lambda
 - 107. Build a Serverless Webpage with API Gateway and Lambda
 - 108. Build an Alexa Skill
 - 109. Serverless Application Model (SAM)
 - 110. Elastic Container Service (ECS)
 - 111. Miscellaneous
-

1. IAM

Question 1:

As an operations administrator, you are running a set of applications hosted on AWS. Your company decided to introduce an API gateway and use it for inter-application co-operation. For this, you need to implement API Gateway permission management and give developers, IT administrators, and users the appropriate level of permissions to manage them.

Select the most appropriate setting method to implement this authority management task.

Options:

- A. Use STS to set access rights to individual users
- B. Use IAM policy to set access rights to individual users
- C. Use AWS Config to set access permissions for individual users
- D. Use the IAM access key to set access privileges for individual users

Answer: B

Explanation:

This scenario asks how to configure API Gateway to give developers, IT administrators, and users permissions to the appropriate level of API. Access to Amazon API Gateway can be controlled by permissions using IAM policies. In order to allow API callers to call APIs, it is necessary to create and set an IAM policy.

Option A is incorrect. STS is a function that gives temporary authentication permission and is not suitable for granting medium-to long-term access authority.

Option C is incorrect. AWS Config does not have the ability to grant permissions.

Option D is incorrect. Privilege management by IAM user or IAM role is required instead of IAM access key

Question 2:

The following IAM policy sets permissions for EC2 instances.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Action": "ec2:*",  
      "Effect": "Allow",  
      "Resource": "*"
```



```

},
{
  "Effect": "Deny",
  "Action": [
    "ec2:*ReservedInstances*",
    "ec2:TerminateInstances"
  ],
  "Resource": "*"
}
]
}

```

Select the correct description for these settings.

Options:

- A. Operations on Reserved instances are allowed
- B. All operations on EC2 instances are allowed
- C. Operations that terminate all EC2 instance types are rejected
- D. Operations that terminate only for all Reserved instances is rejected

Answer: C

Explanation

This IAM policy allows all EC2 actions, but prohibits “all operations on Reserved Instances” and “terminate operations on all instances”.

The first half of the statement gives permission for all EC2. This is a full access right.

```

{
  "Action": "ec2:*",
  "Effect": "Allow",
  "Resource": "*"
},
```

In the second half of the statement, it is set to reject only “All actions of Reserved Instances” and “Actions to terminate all EC2 instances”.

```

"Effect": "Deny",
"Action": [
  "ec2:*ReservedInstances*",
  "ec2:TerminateInstances"
],
"Resource": "*"
```

As a result, with this setting, “any action for Reserved Instances” and “instance termination processing for all EC2 instances” cannot be performed, and Option 3 is the correct answer.

Question 3:

As a Solutions Architect, you plan to use SQS queues and Lambda to take advantage of serverless configurations in the AWS cloud. In this configuration, the SQS queue runs Lambda in parallel and then stores the data in DynamoDB.

Select the settings you need in order to send messages using Lambda.

Options:

- A. Need to use FIFO queue
- B. Integrate Lambda functions with API Gateway
- C. Set the IAM role to a Lambda function
- D. Set security group to Lambda function

Answer: C

Explanation

If your Lambda function needs to access other AWS resources, your Lambda function must have an IAM role that grants access to that service. This time the Lambda function needs access to SQS. Therefore, option 3 is the correct answer.

Use the IAM role for Lambda permissions. To grant permissions to other accounts that use your Lambda resource ↑ to grant permissions to other AWS resources, set the policy that applies to the resource itself in your IAM role.

Your Amazon SQS role must include the following permissions:

lambda: CreateEventSourceMapping
lambda: ListEventSourceMappings
lambda: ListFunctions
The lambda execution role must include the following permissions:

sqs: DeleteMessage
sqs: GetQueueAttributes
sqs: ReceiveMessage

If you want to associate an encrypted queue with your Lambda function, add the kms: Decrypt permission to your Lambda execution role.

Option 1 is incorrect. Standard queues are also available for SQS queues.

Option 2 is incorrect. You don't need to integrate your Lambda function with API Gateway because it executes your Lambda function triggered by an SQS queue.

Option 4 is incorrect. You don't need to set the security group in your Lambda function.

Question 4:

A developer created an application that uses Amazon EC2 and an Amazon RDS MySQL database instance. The developer stored the database user name and password in a configuration file on the root EBS volume of the EC2 application instance. A Solutions Architect has been asked to design a more secure solution.

What should the Solutions Architect do to achieve this requirement?

Options:

- A. Attach an additional volume to the EC2 instance with encryption enabled. Move the configuration file to the encrypted volume
- B. Install an Amazon-trusted root certificate on the application instance and use SSL/TLS encrypted connections to the database
- C. Move the configuration file to an Amazon S3 bucket. Create an IAM role with permission to the bucket and attach it to the EC2 instance
- D. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance

Answer: D

Explanation

The key problem here is having plain text credentials stored in a file. Even if you encrypt the volume there is still a security risk as the credentials are loaded by the application and passed to RDS.

The best way to secure this solution is to get rid of the credentials completely by using an IAM role instead. The IAM role can be assigned permissions to the database instance and can be attached to the EC2 instance. The instance will then obtain temporary security credentials from AWS STS which is much more secure.

CORRECT: “Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance” is the correct answer.

INCORRECT: “Move the configuration file to an Amazon S3 bucket. Create an IAM role with permission to the bucket and attach it to the EC2 instance” is incorrect. This just relocates the file; the contents are still unsecured and must be loaded by the application and passed to RDS. This is an insecure process.

INCORRECT: “Attach an additional volume to the EC2 instance with encryption enabled. Move the configuration file to the encrypted volume” is incorrect. This will only encrypt the file at rest, it still must be read, and the contents passed to RDS which is insecure.

INCORRECT: “Install an Amazon-trusted root certificate on the application instance and use SSL/TLS encrypted connections to the database” is incorrect. The file is still unsecured on the EBS volume so encrypting the credentials in an encrypted channel between the EC2 instance and RDS does not solve all security issues.

Question 5:

A company requires that all AWS IAM user accounts have specific complexity requirements and minimum password length.

How should a Solutions Architect accomplish this?

Options:

- A. Set a password policy for each IAM user in the AWS account
- B. Create an IAM policy that enforces the requirements and apply it to all users
- C. Set a password policy for the entire AWS account
- D. Use an AWS config rule to enforce the requirements when creating user accounts.

Answer: C

Explanation

The easiest way to enforce this requirement is to update the password policy that applies to the entire AWS account. When you create or change a password policy, most of the password policy settings are enforced the next time your users change their passwords. However, some of the settings are enforced immediately such as the password expiration period.

CORRECT: “Set a password policy for the entire AWS account” is the correct answer.

INCORRECT: “Set a password policy for each IAM user in the AWS account” is incorrect. There’s no need to set an individual password policy for each user, it will be easier to set the policy for everyone.

INCORRECT: “Create an IAM policy that enforces the requirements and apply it to all users” is incorrect. As there is no specific targeting required it is easier to update the account password policy.

INCORRECT: “Use an AWS Config rule to enforce the requirements when creating user accounts” is incorrect. You cannot use AWS Config to enforce the password requirements at the time of creating a user account.

Question 6:

An organization wants to delegate access to a set of users from the development environment so that they can access some resources in the production environment which is managed under another AWS account.

As a solutions architect, which of the following steps would you recommend?

Options:

- A. Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment
- B. Both IAM roles and IAM users can be used interchangeably for cross-account access
- C. It is not possible to access cross-account resources
- D. Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume this IAM role while accessing the resources from the production environment

Answer: D

Explanation

Correct option:

Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume this IAM role while accessing the resources from the production environment

IAM roles allow you to delegate access to users or services that normally don’t have access to your organization’s AWS resources. IAM users or AWS services can assume a role to obtain temporary security credentials that can be used to make AWS API calls. Consequently, you don’t have to share long-term credentials for access to a resource. Using IAM roles, it is possible to access cross-account resources.

Incorrect options:

Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment – There is no need to create new IAM user credentials for the production environment, as you can use IAM roles to access cross-account resources.

It is not possible to access cross-account resources – You can use IAM roles to access cross-account resources.

Both IAM roles and IAM users can be used interchangeably for cross-account access – IAM roles and IAM users are separate IAM entities and should not be mixed. Only IAM roles can be used to access cross-account resources.

Question 7:

A large IT company wants to federate its workforce into AWS accounts and business applications.

Which of the following AWS services can help build a solution for this requirement? (Select two)

Options:

- A. Use AWS Organizations
- B. Use Multi-Factor Authentication
- C. Use AWS Identity and Access Management(IAM)
- D. Use AWS Security Token Service (AWS STS) to get temporary security credentials
- E. Use AWS Single Sign-On(SSO)

Answer: C & E

Explanation

Correct options:

Use AWS Single Sign-On (SSO)

Use AWS Identity and Access Management (IAM)

Identity federation is a system of trust between two parties for the purpose of authenticating users and conveying the information needed to authorize their access to resources. In this system, an identity provider (IdP) is responsible for user authentication, and a service provider (SP), such as a service or an application, controls access to resources. By administrative agreement and configuration, the SP trusts the IdP to authenticate users and relies on the information provided by the IdP about them. After authenticating a user, the IdP sends the SP a message, called an assertion, containing the user's sign-in name and other attributes that the SP needs to establish a session with the user and to determine the scope of resource access that the SP should grant. Federation is a common approach to building access control systems that manage users centrally within a central IdP and govern their access to multiple applications and services acting as SPs.

You can use two AWS services to federate your workforce into AWS accounts and business applications: AWS Single Sign-On (SSO) or AWS Identity and Access Management (IAM). AWS SSO is a great choice to help you define federated access permissions for your users based on their group memberships in a single centralized directory. If you use multiple directories or want to manage the permissions based on user attributes, consider AWS IAM as your design alternative.

Incorrect options:

Use Multi-Factor Authentication – AWS multi-factor authentication (AWS MFA) provides an extra level of security that you can apply to your AWS environment. You can enable AWS MFA for your AWS account and for individual AWS Identity and Access Management (IAM) users you create under your account. MFA added another layer of security to IAM and is not a stand-alone service.

Use AWS Security Token Service (AWS STS) to get temporary security credentials – Temporary security credentials consist of the AWS access key ID, secret access key, and security token. Temporary security credentials are valid for a specified duration and for a specific set of permissions. If you're making direct HTTPS API requests to AWS, you can sign those requests with the temporary security credentials that you get from AWS Security Token Service (AWS STS). STS is not a federation service.

Use AWS Organizations – AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. AWS Organizations includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business. It does not offer federation capability, as is needed in the use case.

Question 8:

An IT company wants to review its security best-practices after an incident was reported where a new developer on the team was assigned full access to DynamoDB. The developer accidentally deleted a couple of tables from the production environment while building out a new feature.

Which is the MOST effective way to address this issue so that such incidents do not recur?

Options:

- A. The CTO should review the permissions for each new developer's IAM user so that such incidents don't recur
- B. Only root user should have full database access in the organization
- C. Use permissions boundary to control the maximum permissions employees can grant to the IAM principals
- D. Remove full database access for all IAM users in the organization

Answer: C

Explanation

Correct option:

Use permissions boundary to control the maximum permissions employees can grant to the IAM principals

A permissions boundary can be used to control the maximum permissions employees can grant to the IAM principals (that is, users and roles) that they create and manage. As the IAM administrator, you can define one or more permissions boundaries using managed policies and allow your employee to create a principal with this boundary. The employee can then attach a permissions policy to this principal. However, the effective permissions of the principal are the intersection of the permissions boundary and permissions policy. As a result, the new principal cannot exceed the boundary that you defined. Therefore, using the permissions boundary offers the right solution for this use-case.

Incorrect options:

Remove full database access for all IAM users in the organization – It is not practical to remove full access for all IAM users in the organization because a select set of users need this access for database administration. So this option is not correct.

The CTO should review the permissions for each new developer's IAM user so that such incidents don't recur – Likewise the CTO is not expected to review the permissions for each new developer's IAM user, as this is best done via an automated procedure. This option has been added as a distractor.

Only root user should have full database access in the organization – As a best practice, the root user should not access the AWS account to carry out any administrative procedures. So this option is not correct.

Question 9:

A development team requires permissions to list an S3 bucket and delete objects from that bucket. A systems administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows the principle of least privilege.

```
"Version": "2021-10-17",
```

```
"Statement": [
```

```
{
```

```
  "Action": [
```

```
    "s3>ListBucket",
```

```
    "s3>DeleteObject"
```

```
],
```

```
  "Resource": [
```

```
    "arn:aws:s3:::example-bucket"
```

```
],
```

```
  "Effect": "Allow"
```

```
}
```

```
]
```

Which statement should a solutions architect add to the policy to address this issue?

Answer:

```
{
```

```
  "Action": [
```

```
    "s3>DeleteObject"
```

```
],
```

```
  "Resource": [
```

```
    "arn:aws:s3:::example-bucket/*"
```

```
],
```

```
  "Effect": "Allow"
```

```
}
```

The main elements of a policy statement are:

Effect: Specifies whether the statement will Allow or Deny an action (Allow is the effect defined here).

Action: Describes a specific action or actions that will either be allowed or denied to run based on the Effect entered. API actions are unique to each service (DeleteObject is the action defined here).

Resource: Specifies the resources—for example, an S3 bucket or objects—that the policy applies to in Amazon Resource Name (ARN) format (example-bucket/* is the resource defined here).

This policy provides the necessary delete permissions on the resources of the S3 bucket to the group.

Question 10:

An IT consultant is helping the owner of a medium-sized business set up an AWS account. What are the security recommendations he must follow while creating the AWS account root user? (Select two)

Options:

A. Encrypt the access keys and save them on Amazon S3

B. Create AWS account root user access keys and share those keys only with the business owner

C. Enable Multi Factor Authentication (MFA) for the AWS account root user account

D. Send an email to the business owner with details of the login username and password for the AWS root user. This will help the business owner to troubleshoot any login issues in future

E. Create a strong password for the AWS account root user

Answer: C & E

Explanation

Correct options:

Create a strong password for the AWS account root user

Enable Multi Factor Authentication (MFA) for the AWS account root user account

Here are some of the best practices while creating an AWS account root user:

1) Use a strong password to help protect account-level access to the AWS Management Console. 2) Never share your AWS account root user password or access keys with anyone. 3) If you do have an access key for your AWS account root user, delete it. If you

must keep it, rotate (change) the access key regularly. You should not encrypt the access keys and save them on Amazon S3. 4) If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. 5) Enable AWS multi-factor authentication (MFA) on your AWS account root user account.

Incorrect options:

Encrypt the access keys and save them on Amazon S3 – AWS recommends that if you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. Even an encrypted access key for the root user poses a significant security risk. Therefore, this option is incorrect.

Create AWS account root user access keys and share those keys only with the business owner – AWS recommends that if you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. Hence, this option is incorrect.

Send an email to the business owner with details of the login username and password for the AWS root user. This will help the business owner to troubleshoot any login issues in future – AWS recommends that you should never share your AWS account root user password or access keys with anyone. Sending an email with AWS account root user credentials creates a security risk as it can be misused by anyone reading the email. Hence, this option is incorrect.

Question 11:

A new DevOps engineer has joined a large financial services company recently. As part of his onboarding, the IT department is conducting a review of the checklist for tasks related to AWS Identity and Access Management.

As a solutions architect, which best practices would you recommend (Select two)?

Options:

- A. Create a minimum number of accounts and share these account credentials among employees
- B. Configure AWS CloudTrail to record all account activity
- C. Enable MFA for privileged users
- D. Grant maximum privileges to avoid assigning privileges again
- E. Use user credentials to provide access specific permissions for Amazon EC2 instances

Answer: B & C

Explanation

Correct options:

Enable MFA for privileged users – As per the AWS best practices, it is better to enable Multi Factor Authentication (MFA) for privileged users via an MFA-enabled mobile device or hardware MFA token.

Configure AWS CloudTrail to record all account activity – AWS recommends to turn on CloudTrail to log all IAM actions for monitoring and audit purposes.

Incorrect options:

Create a minimum number of accounts and share these account credentials among employees – AWS recommends that user account credentials should not be shared between users. So, this option is incorrect.

Grant maximum privileges to avoid assigning privileges again – AWS recommends granting the least privileges required to complete a certain job and avoid giving excessive privileges which can be misused. So, this option is incorrect.

Use user credentials to provide access specific permissions for Amazon EC2 instances – It is highly recommended to use roles to grant access permissions for EC2 instances working on different AWS services. So, this option is incorrect.

Question 17: Skipped

What does this IAM policy do?

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "NotIpAddress": [
            "192.168.1.1/32"
          ]
        }
      }
    }
  ]
}
```

```

"aws:SourceIp": "34.50.31.0/24"
}
}
}
]
}

```

- It allows starting EC2 instances only when they have a Public IP within the 34.50.31.0/24 CIDR block
- It allows starting EC2 instances only when the IP where the call originates is within the 34.50.31.0/24 CIDR block (Correct)
- It allows starting EC2 instances only when they have a Private IP within the 34.50.31.0/24 CIDR block
- It allows starting EC2 instances only when they have an Elastic IP within the 34.50.31.0/24 CIDR block

Explanation

Correct option:

It allows starting EC2 instances only when the IP where the call originates is within the 34.50.31.0/24 CIDR block

You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, ACLs, and session policies.

Consider the following snippet from the given policy document:

```

"Condition": {
  "IpAddress": {
    "aws:SourceIp": "34.50.31.0/24"
  }
}

```

The aws:SourceIP in this condition always represents the IP of the caller of the API. That is very helpful if you want to restrict access to certain AWS API for example from the public IP of your on-premises infrastructure.

Please see this overview of Elastic vs Public vs Private IP addresses:

Elastic IP address – An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.

Private IP address – A private IPv4 address is an IP address that's not reachable over the Internet. You can use private IPv4 addresses for communication between instances in the same VPC.

Public IP address – A public IP address is an IPv4 address that's reachable from the Internet. You can use public addresses for communication between your instances and the Internet.

Please note 34.50.31.0/24 is a public IP range, not a private IP range. Private IP ranges are: 192.168.0.0 – 192.168.255.255 (65,536 IP addresses) 172.16.0.0 – 172.31.255.255 (1,048,576 IP addresses) 10.0.0.0 – 10.255.255.255 (16,777,216 IP addresses)

Incorrect options:

It allows starting EC2 instances only when they have a Public IP within the 34.50.31.0/24 CIDR block

It allows starting EC2 instances only when they have an Elastic IP within the 34.50.31.0/24 CIDR block

It allows starting EC2 instances only when they have a Private IP within the 34.50.31.0/24 CIDR block

Each of these three options suggests that the IP addresses of the EC2 instances must belong to the 34.50.31.0/24 CIDR block for the EC2 instances to start. Actually, the policy states that the EC2 instance should start only when the IP where the call originates is within the 34.50.31.0/24 CIDR block. Hence these options are incorrect.

Question 32:

What does this IAM policy do?

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ]
    }
  ]
}

```

```

    },
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:RequestedRegion": "eu-west-1"
        }
    }
}
]
}

```

- A• It allows running EC2 instances in any region when the API call is originating from the eu-west-1 region
- B• It allows running EC2 instances anywhere but in the eu-west-1 region
- C• It allows to run EC2 instances in the eu-west-1 region, when the API call is made from the eu-west-1 region
- D• It allows running EC2 instances only in the eu-west-1 region, and the API call can be made from anywhere in the world

Answer: D

Explanation

Correct option:

It allows running EC2 instances only in the eu-west-1 region, and the API call can be made from anywhere in the world. You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, ACLs, and session policies.

You can use the aws:RequestedRegion key to compare the AWS Region that was called in the request with the Region that you specify in the policy. You can use this global condition key to control which Regions can be requested.

aws:RequestedRegion represents the target of the API call. So in this example, we can only launch EC2 instances in eu-west-1, and we can do this API call from anywhere.

Incorrect options:

It allows running EC2 instances anywhere but in the eu-west-1 region

It allows running EC2 instances in any region when the API call is originating from the eu-west-1 region

It allows running EC2 instances in the eu-west-1 region when the API call is made from the eu-west-1 region

These three options contradict the earlier details provided in the explanation. To summarize, aws:RequestedRegion represents the target of the API call. So, we can only launch EC2 instances in eu-west-1 region and we can do this API call from anywhere. Hence these options are incorrect.

Question 35:

You have a team of developers in your company, and you would like to ensure they can quickly experiment with AWS Managed Policies by attaching them to their accounts, but you would like to prevent them from doing an escalation of privileges, by granting themselves the AdministratorAccess managed policy. How should you proceed?

- A• Attach an IAM policy to your developers, that prevents them from attaching the AdministratorAccess policy
- B• Create a Service Control Policy (SCP) on your AWS account that restricts developers from attaching themselves the AdministratorAccess policy
- C• For each developer, define an IAM permission boundary that will restrict the managed policies they can attach to themselves
- D• Put the developers into an IAM group, and then define an IAM permission boundary on the group that will restrict the managed policies they can attach to themselves

Answer: C

Explanation

Correct option:

For each developer, define an IAM permission boundary that will restrict the managed policies they can attach to themselves. AWS supports permissions boundaries for IAM entities (users or roles). A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity ↑ rmissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. Here we have to use an IAM permission boundary. They can only be applied to roles or users, not IAM groups.

Incorrect options:

Create a Service Control Policy (SCP) on your AWS account that restricts developers from attaching themselves the AdministratorAccess policy – Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled. SCPs aren't available if your organization has enabled only the consolidated billing features. Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a guardrail for what actions the principals can perform. If you consider this option, since AWS Organizations is not mentioned in this question, so we can't apply an SCP.

Attach an IAM policy to your developers, that prevents them from attaching the AdministratorAccess policy – This option is incorrect as the developers can remove this policy from themselves and escalate their privileges.

Put the developers into an IAM group, and then define an IAM permission boundary on the group that will restrict the managed policies they can attach to themselves – IAM permission boundary can only be applied to roles or users, not IAM groups. Hence this option is incorrect.

Question 38:

You would like to store a database password in a secure place, and enable automatic rotation of that password every 90 days.

What do you recommend?

- A• Key Management Service (KMS)
- B• CloudHSM
- C• Secrets Manager
- D• SSM Parameter Store

Answer: C

Explanation**Correct option:**

“Secrets Manager”

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. The correct answer here is Secrets Manager

Incorrect options:

“KMS” – AWS Key Management Service (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud. When you use server-side encryption with AWS KMS (SSE-KMS), you can specify a customer-managed CMK that you have already created. SSE-KMS provides you with an audit trail that shows when your CMK was used and by whom. KMS is an encryption service, it's not a secrets store. So this option is incorrect.

“CloudHSM” – AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your encryption keys on the AWS Cloud. With CloudHSM, you can manage your encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM is standards-compliant and enables you to export all of your keys to most other commercially-available HSMs, subject to your configurations. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups.

CloudHSM is also an encryption service, not a secrets store. So this option is incorrect.

“SSM Parameter Store” – AWS Systems Manager Parameter Store (aka SSM Parameter Store) provides secure, hierarchical storage for configuration data management and secrets management. You can store data such as passwords, database strings, EC2 instance IDs, Amazon Machine Image (AMI) IDs, and license codes as parameter values. You can store values as plain text or encrypted data. You can reference Systems Manager parameters in your scripts, commands, SSM documents, and configuration and automation workflows by using the unique name that you specified when you created the parameter.

SSM Parameter Store can serve as a secrets store, but you must rotate the secrets yourself, it doesn't have an automatic capability for this. So this option is incorrect.



3. S3

Question 1:

Your company is designing a web application that stores static content in an Amazon S3 bucket. As a non-functional requirement of the application, this bucket must handle more than 150 PUT requests per second quickly.

What should you do to ensure optimal performance?

Options:

- A. Use a random prefix for object key name
- B. Use a prefix such as date for object key name
- C. Use a multi part upload
- D. Enable S3 lifecycle rule

Answer: B

Explanation:

Option B is the correct answer. Amazon S3 can automatically improve performance so that it can support at least 3,500 requests / second when adding data with existing settings, and it can support 5,500 requests / second when retrieving data. Previously, performance improvements with the S3 prefix were essential for S3 to deliver this performance, but S3's existing settings can now support request rates.

Option 1 is incorrect. This setting was previously correct, but with improved S3 request rate performance, you no longer need to set the object prefix to random.

Option 3 is incorrect. Multipart upload is a feature used when uploading large files to S3 and has no effect on this requirement.

Option 4 is incorrect. S3 lifecycle rules have nothing to do with improving processing performance.

Question 2:

Your company wants to use AWS as a mechanism for managing their documents. Documents stored by your company may be used frequently in the early stages, but after four months they will be used less frequently, so you will need to archive the documents appropriately.

Which AWS service settings do you need to configure to meet this requirement?

Options:

- A. Set a life cycle rule to store data in EBS and move to S3 after 4 months
- B. Set a life cycle rule to store data in S3 Standard and move to Glacier after 4 months
- C. Set a life cycle rule to store data in EFS and move to Glacier after 4 months
- D. Set a life cycle rule to store data in S3 RRS and move to Glacier after 4 months

Answer: B

Explanation:

Documents are stored in S3, and the life cycle policy is set to move to a storage type with lower cost.

In the early stages, documents are accessed frequently, so you need a storage type with suitable access efficiency, like S3 Standard. After that, it is common to use Glacier (or Glacier deep archive) as storage for long-term storage.

Question 3:

The following bucket policy sets permissions for S3 buckets.

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "NotIpAddress": {"aws:SourceIp": "54.240.143.0/24"}
      }
    }
  ]
}
```



```
]  
}  
Select the correct description of this setting.
```

Options:

- A. All actions from the specified IP address range can be performed on this S3 bucket
- B. All actions can be performed on this S3 bucket from outside the specified IP address range
- C. Access to this S3 bucket from the specified IP address range is denied
- D. Access to this S3 bucket from outside of the specified IP address range is denied

Answer: D

Explanation

In this bucket policy, the first half of the statement denies all actions from all users to the example bucket.

```
"Effect": "Deny",  
"Principal": "*",  
"Action": "s3:*",  
"Resource": "arn:aws:s3:::examplebucket/*",
```

The latter statement specifies 54.240.143.0/24 as a condition for the allowed IP address range. The Condition block uses the NotIpAddress condition and aws: SourceIp. Since the NotIpAddress condition is used here, it means that IP addresses other than 54.240.143.0/24 are affected by this policy.

```
"Condition": {  
    "NotIpAddress": {"aws:SourceIp": "54.240.143.0/24"}  
}
```

Therefore, access to objects in this S3 bucket is denied if the request to this bucket is from an IP outside of the specified IP address range. Therefore, option 4 is the correct answer.

Question 4:

You have set up S3 for your data management application. This application makes several requests, including read / write and update, on objects in the S3 bucket.

If you update an object with the same key name, how will the updated object be reflected on? E.g will there be any error/discrepancies in the object upon inspection after update?

Options:

- A. Since S3 uses eventual consistency models, there may be differences when reflecting data
- B. Since S3 uses eventual consistency models, there is no difference when reflecting data
- C. Since S3 uses strong consistency models, there may be differences when reflecting data
- D. Since S3 uses strong consistency models, there is no difference when reflecting data

Answer: D

Explanation

Option 4 is the correct answer. S3 utilizes a strong consistency model, so there are no errors in reflection. Before December 2020, S3 used an eventual consistency model. If an update was made on an object with the same key name as the original object, the read request immediately after might not reflect the updated object. However, S3 now uses a strong consistency model, so these discrepancies no longer occur.

S3 adopted the “strong consistency model” for data registration / update / deletion.

Options 1 and 2 are incorrect. S3 used an eventual consistency model, but recently it has improved to a strong consistency model.

Option 3 is incorrect. S3 now utilizes a strong consistency model, which eliminates the possibility of reflection errors.

Question 5:

Your company uses a business application hosted on AWS to manage records related to daily business. According to industry regulations, recorded data must be retained for 5 years. Most of these archives are rarely accessed, but data must be provided within 24 hours in response to an audit request.

Which of the following storage should you choose as the most cost-effective storage?

Options:

- A. Amazon Glacier (standard retrieval)
- B. Amazon S3 Glacier Deep Archive
- C. S3 Standard

D. S3 One Zone IA

E. S3 Standard IA

Answer: B

Explanation

Option 2 is the correct answer. In this scenario, storage requirements are cost-effective to store data over the medium to long term and extract data within 24 hours. The Glacier Deep Archive storage class is designed to offer durable, secure, high-volume data storage at the lowest prices on AWS. Data is stored across three or more of his AWS Availability Zones and can be retrieved within 12 hours.

Option 1 is incorrect. Glacier is cheap and suitable for long-term storage of data, but it is a storage that takes several hours to acquire data. Data can be acquired in about 1 to 5 minutes by using quick reading. However, the Glacier Deep Archive storage class is cheaper than Glacier.

Option 3 is incorrect. S3 Standard is the most costly data storage in S3 and does not meet this requirement.

Option 4 is incorrect. S3 One Zone-IA saves money by storing infrequently accessed data in a single, less resilient, Availability Zone. However, the Glacier Deep Archive storage class is cheaper than the S3 One Zone-IA.

Option 5 is incorrect. Standard-IA is for infrequent access, but it can be read quickly, so it can be used suddenly. However, the Glacier Deep Archive storage class is cheaper than Standard-IA.

Question 6:

As a Solutions Architect, you use AWS to build solutions for managing and storing corporate documents. Once the data is saved, it is rarely used, but it is required to be obtained within 10 hours according to the administrator's instructions if necessary. You have decided to use Amazon Glacier and are considering how to set it up.

How should you set the data acquisition method for Glacier?

Options:

A. Expedited retrievals

B. Standard retrievals

C. Bulk retrievals

D. Vault lock

Explanation

Glacier's standard retrieval is the optimal setting because of the requirement to retrieve the data within 10 hours according to the administrator's instructions as needed. With standard retrieval, you can access all archives within 3-5 hours. Therefore, option 2 is the correct answer.

Option 1 is incorrect. Glacier's Expedited retrievals gives you quick access to your data if you need a subset of your archives quickly. For all archives except the largest archives (250 MB and above), the data accessed with Expedited retrievals is typically available within 1-5 minutes. However, Expedited retrievals are not cost-optimal or preferred in this situation.

Option 3 is incorrect. Bulk retrievals is Glacier's cheapest retrieval option, which allows you to retrieve large amounts of data (including petabytes of data) within a day. Bulk retrievals typically takes 5-12 hours, so data acquisition cannot be completed within 10 hours.

Option 4 is incorrect. Glacier vault locks allow you to easily deploy and apply compliance management for each Glacier vault using vault lock policies. Specify a control such as write once read many (WORM) in the vault lock policy to lock the policy so that it cannot be edited in the future. This feature is irrelevant to this requirement.

Question 7:

Your company develops and operates an application that provides image data in the public domain. The image data is stored in S3, and the application temporarily displays it in response to the user's request. This image should be protected so that it is only available to specific users.

What mechanism do I need to use to meet this requirement?

Options:

A. Distribute images with a time-limited pre-signed URL

B. Image distribution by CloudFront distribution

C. Protect your images with an encryption key

D. Limit users by switching to EFS image sharing

Explanation

If you create a pre-signed URL and have permissions to the object, only the user who has the pre-signed URL can access the object. By using this function, the application can grant a specific user permission to the target image for a limited time.

Therefore, option 1 is the correct answer.

Option 2 is wrong. It is not possible to limit the users to whom images are delivered to using CloudFront delivery settings alone.

It is necessary to use signed URLs and signed cookies in CloudFront.

Option 3 is wrong. There is no setting that allows a specific user to share images with an encryption key.

Option 4 is wrong. EFS is a storage that allows data sharing between instances, but it cannot be accessed by a third party via the Internet. Therefore, it is more appropriate to use S3 as a storage service for showing data to the outside.

Question 8:

Some companies store employee user profiles and access logs in S3. As this data is uploaded and modified on a daily basis, there is a concern that users may accidentally delete objects in their S3 bucket. Therefore, it is necessary to take preventive measures, but it should not affect the business.

Choose the best way to prevent accidental deletion of objects in your S3 bucket (Select two)

Options:

- A. Enable the versioning feature on S3 bucket
- B. Enable encryption in S3 bucket
- C. Enable MFA authentication on S3 bucket
- D. Set data deletion not possible for S3 bucket
- E. Set deletion refusal by IAM role in S3 bucket

Answer: A & C

Explanation

By enabling MFA authentication for your S3 bucket, users will be required to perform MFA authentication every time they try to perform a deletion process, which will prevent deletion due to operational mistakes. Furthermore, you can restore deleted files by enabling the versioning function. Therefore, options 1 and 3 are correct.

Option 2 is incorrect. You can increase data protection by enabling encryption in your S3 bucket, but it does not prevent data loss.

Option 4 is incorrect. The S3 bucket can be configured so that objects cannot be deleted by default, but this is only available during initial setup. You can't change the settings of an S3 bucket that you're already using. In addition, there are cases where data deletion operations are required, which is inappropriate in this case.

Option 5 is incorrect. Access permissions must be set by the IAM user, not the IAM role.

Question 9:

A video production company is planning to move some of its workloads to the AWS Cloud. The company will require around 5 TB of storage for video processing with the maximum possible I/O performance. They also require over 400 TB of extremely durable storage for storing video files and 800 TB of storage for long-term archival.

Which combinations of services should a Solutions Architect use to meet these requirements?

Options:

- A. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage
- B. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
- C. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage
- D. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Answer: B

Explanation

The best I/O performance can be achieved by using instance store volumes for the video processing. This is safe to use for use cases where the data can be recreated from the source files so this is a good use case.

For storing data durably Amazon S3 is a good fit as it provides 99.999999999% of durability. For archival the video files can then be moved to Amazon S3 Glacier which is a low cost storage option that is ideal for long-term archival.

CORRECT: “Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage” is the correct answer.

INCORRECT: “Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage” is incorrect. EBS is not going to provide as much I/O performance as an instance store volume so is not the best choice for this use case.

INCORRECT: “Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and

↑ on S3 for

archival storage" is incorrect. EFS does not provide as much durability as Amazon S3 and will not be as cost-effective.

INCORRECT: "Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage" is incorrect. EBS and EFS are not the best choices here as described above.

Question 10:

A company has uploaded some highly critical data to an Amazon S3 bucket. Management are concerned about data availability and require that steps are taken to protect the data from accidental deletion. The data should still be accessible, and a user should be able to delete the data intentionally.

Which combination of steps should a solutions architect take to accomplish this? (Select TWO.)

Options:

- A. Enable MFA delete on the S3 bucket
- B. Create a bucket policy on the S3 bucket
- C. Enable default encryption on the S3 bucket
- D. Enable versioning on the S3 bucket
- E. Create a lifecycle policy for the objects in the S3 bucket

Answer: A & D

Explanation

Multi-factor authentication (MFA) delete adds an additional step before an object can be deleted from a versioning-enabled bucket.

With MFA delete the bucket owner must include the x-amz-mfa request header in requests to permanently delete an object version or change the versioning state of the bucket.

CORRECT: "Enable versioning on the S3 bucket" is a correct answer.

CORRECT: "Enable MFA Delete on the S3 bucket" is also a correct answer.

INCORRECT: "Create a bucket policy on the S3 bucket" is incorrect. A bucket policy is not required to enable MFA delete.

INCORRECT: "Enable default encryption on the S3 bucket" is incorrect. Encryption does protect against deletion.

INCORRECT: "Create a lifecycle policy for the objects in the S3 bucket" is incorrect. A lifecycle policy will move data to another storage class but does not protect against deletion.

Question 11:

A solutions architect is creating a document submission application for a school. The application will use an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to upload and modify the documents.

Which combination of actions should be taken to meet these requirements? (Select TWO.)

Options:

- A. Enable MFA delete on the bucket
- B. Encrypt the bucket using AWS SSE-S3
- C. Set read-only permissions on the bucket
- D. Attach an IAM policy to the bucket
- E. Enable versioning on the bucket

Answer: A & E

Explanation

None of the options present a good solution for specifying permissions required to write and modify objects so that requirement needs to be taken care of separately. The other requirements are to prevent accidental deletion and the ensure that all versions of the document are available.

The two solutions for these requirements are versioning and MFA delete. Versioning will retain a copy of each version of the document and multi-factor authentication delete (MFA delete) will prevent any accidental deletion as you need to supply a second factor when attempting a delete.

CORRECT: "Enable versioning on the bucket" is a correct answer.

CORRECT: "Enable MFA Delete on the bucket" is also a correct answer.

INCORRECT: "Set read-only permissions on the bucket" is incorrect as this will also prevent any writing to the bucket which is not desired.

INCORRECT: "Attach an IAM policy to the bucket" is incorrect as users need to modify documents which will also allow deletion. Therefore, a method must be implemented to just control deletes.

INCORRECT: "Encrypt the bucket using AWS SSE-S3" is incorrect as encryption doesn't stop you from deleting an object.

Question 12:

A team are planning to run analytics jobs on log files each day and require a storage solution. The size and number of logs is unknown and data will persist for 24 hours only.

What is the MOST cost-effective solution?

Options:

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

Answer: B

Explanation

S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object.

CORRECT: “Amazon S3 Standard” is the correct answer.

INCORRECT: “Amazon S3 Intelligent-Tiering” is incorrect as there is an additional fee for using this service and for a short-term requirement it may not be beneficial.

INCORRECT: “Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)” is incorrect as this storage class has a minimum capacity charge per object (128 KB) and a per GB retrieval fee.

INCORRECT: “Amazon S3 Glacier Deep Archive” is incorrect as this storage class is used for archiving data. There are retrieval fees and it takes hours to retrieve data from an archive.

Question 13:

A solutions architect needs to backup some application log files from an online ecommerce store to Amazon S3. It is unknown how often the logs will be accessed or which logs will be accessed the most. The solutions architect must keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

Options:

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

Answer: A

Explanation

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead.

It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. This is an ideal use case for intelligent-tiering as the access patterns for the log files are not known.

CORRECT: “S3 Intelligent-Tiering” is the correct answer.

INCORRECT: “S3 Standard-Infrequent Access (S3 Standard-IA)” is incorrect as if the data is accessed often retrieval fees could become expensive.

INCORRECT: “S3 One Zone-Infrequent Access (S3 One Zone-IA)” is incorrect as if the data is accessed often retrieval fees could become expensive.

INCORRECT: “S3 Glacier” is incorrect as if the data is accessed often retrieval fees could become expensive. Glacier also requires more work in retrieving the data from the archive and quick access requirements can add further costs.

Question 14:

Which of the following features of an Amazon S3 bucket can only be suspended once they have been enabled?

Options:

- A. Static Website Hosting
- B. Versioning
- C. Server Access Logging
- D. Requester Pays



Answer: B

Explanation

Correct option:

Versioning

Once you version-enable a bucket, it can never return to an unversioned state. Versioning can only be suspended once it has been enabled.

Incorrect options:

Server Access Logging

Static Website Hosting

Requester Pays

Server Access Logging, Static Website Hosting and Requester Pays features can be disabled even after they have been enabled.

Question 15:

A healthcare startup needs to enforce compliance and regulatory guidelines for objects stored in Amazon S3. One of the key requirements is to provide adequate protection against accidental deletion of objects.

As a solutions architect, what are your recommendations to address these guidelines? (Select two)

Options:

- A. Establish a process to get managerial approval for deleting S3 objects
- B. Create an event trigger on deleting any S3 object. The event invokes an SNS notification via email to the IT manager
- C. Enable versioning on the bucket
- D. Change the configuration on AWS S3 console so that the user needs to provide additional confirmation while deleting any S3 object
- E. Enable MFA delete on the bucket

Answer: C & E

Explanation

Correct options:

Enable versioning on the bucket – Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite.

For example:

If you overwrite an object, it results in a new object version in the bucket. You can always restore the previous version. If you delete an object, instead of removing it permanently, Amazon S3 inserts a delete marker, which becomes the current object version. You can always restore the previous version. Hence, this is the correct option.

Enable MFA delete on the bucket – To provide additional protection, multi-factor authentication (MFA) delete can be enabled. MFA delete requires secondary authentication to take place before objects can be permanently deleted from an Amazon S3 bucket. Hence, this is the correct option.

Incorrect options:

Create an event trigger on deleting any S3 object. The event invokes an SNS notification via email to the IT manager – Sending an event trigger after object deletion does not meet the objective of preventing object deletion by mistake because the object has already been deleted. So, this option is incorrect.

Establish a process to get managerial approval for deleting S3 objects – This option for getting managerial approval is just a distractor.

Change the configuration on AWS S3 console so that the user needs to provide additional confirmation while deleting any S3 object – There is no provision to set up S3 configuration to ask for additional confirmation before deleting an object. This option is incorrect.

Question 34:

An audit department generates and accesses the audit reports only twice in a financial year. The department uses AWS Step Functions to orchestrate the report creating process that has failover and retry scenarios built into the solution. The underlying data to create these audit reports is stored on S3, runs into hundreds of Terabytes and should be available with millisecond latency.

As a solutions architect, which is the MOST cost-effective storage class that you would recommend to be used for this use-case?

Options:

- A. Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

- B. Amazon S3 Glacier (S3 Glacier)
- C. Amazon S3 Standard
- D. Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

Answer: A

Explanation

Correct option:

Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

Since the data is accessed only twice in a financial year but needs rapid access when required, the most cost-effective storage class for this use-case is S3 Standard-IA. S3 Standard-IA storage class is for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA matches the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. Standard-IA is designed for 99.9% availability compared to 99.99% availability of S3 Standard. However, the report creation process has failover and retry scenarios built into the workflow, so in case the data is not available owing to the 99.9% availability of S3 Standard-IA, the job will be auto re-invoked till data is successfully retrieved. Therefore this is the correct option.

Incorrect options:

Amazon S3 Standard – S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. As described above, S3 Standard-IA storage is a better fit than S3 Standard, hence using S3 standard is ruled out for the given use-case.

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) – The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. S3 Standard-IA matches the high durability, high throughput, and low latency of S3 Intelligent-Tiering, with a low per GB storage price and per GB retrieval fee. Moreover, Standard-IA has the same availability as that of S3 Intelligent-Tiering. So, it's cost-efficient to use S3 Standard-IA instead of S3 Intelligent-Tiering.

Amazon S3 Glacier (S3 Glacier) – S3 Glacier on the other hand, is a secure, durable, and low-cost storage class for data archiving. S3 Glacier cannot support millisecond latency, so this option is ruled out.

Question 35:

The IT department at a consulting firm is conducting a training workshop for new developers. As part of an evaluation exercise on Amazon S3, the new developers were asked to identify the invalid storage class lifecycle transitions for objects stored on S3.

Can you spot the INVALID lifecycle transitions from the options below? (Select two)

Options:

- A. S3 Intelligent-Tiering => S3 Standard
- B. S3 One Zone-IA => S3 Standard-IA
- C. S3 Standard => S3 Intelligent-Tiering
- D. S3 Standard-IA => S3 Intelligent-Tiering
- E. S3 Standard-IA => S3 One Zone-IA

Answer: A & B

Explanation

Correct options:

As the question wants to know about the INVALID lifecycle transitions, the following options are the correct answers –

S3 Intelligent-Tiering => S3 Standard

S3 One Zone-IA => S3 Standard-IA

Following are the unsupported life cycle transitions for S3 storage classes – Any storage class to the S3 Standard storage class. Any storage class to the Reduced Redundancy storage class. The S3 Intelligent-Tiering storage class to the S3 Standard-IA storage class. The S3 One Zone-IA storage class to the S3 Standard-IA or S3 Intelligent-Tiering storage classes.

Incorrect options:

S3 Standard => S3 Intelligent-Tiering

S3 Standard-IA => S3 Intelligent-Tiering

S3 Standard-IA => S3 One Zone-IA

Here are the supported life cycle transitions for S3 storage classes – The S3 Standard storage class to any other storage class. Any storage class to the S3 Glacier or S3 Glacier Deep Archive storage classes. The S3 Standard-IA storage class to the S3 Intelligent-Tiering or S3 One Zone-IA storage classes. The S3 Intelligent-Tiering storage class to the S3 One Zone-IA storage class. The S3 Glacier storage class to the S3 Glacier Deep Archive storage class.

Question 36:

A media agency stores its re-creatable assets on Amazon S3 buckets. The assets are accessed by a large number of users for the first few days and the frequency of access falls down drastically after a week. Although the assets would be accessed occasionally after the first week, but they must continue to be immediately accessible when required. The cost of maintaining all the assets on S3 storage is turning out to be very expensive and the agency is looking at reducing costs as much as possible.

As a Solutions Architect, can you suggest a way to lower the storage costs while fulfilling the business requirements?

- A. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days
- B. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days
- C. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days
- D. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days

Answer: B

Explanation

Correct option:

Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days – S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed and re-creatable data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. The minimum storage duration is 30 days before you can transition objects from S3 Standard to S3 One Zone-IA.

S3 One Zone-IA offers the same high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. S3 Storage Classes can be configured at the object level, and a single bucket can contain objects stored across S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can also use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.

Incorrect options:

Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days

Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days

As mentioned earlier, the minimum storage duration is 30 days before you can transition objects from S3 Standard to S3 One Zone-IA or S3 Standard-IA, so both these options are added as distractors.

Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days – S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files. But, it costs more than S3 One Zone-IA because of the redundant storage across availability zones. As the data is re-creatable, so you don't need to incur this additional cost.

Question 37:

A file-hosting service uses Amazon S3 under the hood to power its storage offerings. Currently all the customer files are uploaded directly under a single S3 bucket. The engineering team has started seeing scalability issues where customer file uploads have started failing during the peak access hours with more than 5000 requests per second.

Which of the following is the MOST resource efficient and cost-optimal way of addressing this issue?

- A. Change the application architecture to create a new S3 bucket for each customer and then upload each customer's files directly under the respective buckets
- B. Change the application architecture to create customer-specific custom prefixes within the single bucket and then upload the daily files into those prefixed locations
- C. Change the application architecture to create a new S3 bucket for each day's data and then upload the daily files directly under that day's bucket
- D. Change the application architecture to use EFS instead of Amazon S3 for storing the customers' uploaded files

Answer: B

Explanation

Correct option:

Change the application architecture to create customer-specific custom prefixes within the single bucket and then upload the daily files into those prefixed locations

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Your applications can easily achieve thousands of transactions per second in request

performance when uploading and retrieving storage from Amazon S3. Amazon S3 automatically scales to high request rates. For example, your application can achieve at least 3,500 PUT/COPY/POST/DELETE or 5,500 GET/HEAD requests per second per prefix in a bucket.

There are no limits to the number of prefixes in a bucket. You can increase your read or write performance by parallelizing reads. For example, if you create 10 prefixes in an Amazon S3 bucket to parallelize reads, you could scale your read performance to 55,000 read requests per second. Please see this example for more clarity on prefixes: if you have a file f1 stored in an S3 object path like so s3://your_bucket_name/folder1/sub_folder_1/f1, then /folder1/sub_folder_1/ becomes the prefix for file f1.

Some data lake applications on Amazon S3 scan millions or billions of objects for queries that run over petabytes of data. These data lake applications achieve single-instance transfer rates that maximize the network interface used for their Amazon EC2 instance, which can be up to 100 Gb/s on a single instance. These applications then aggregate throughput across multiple instances to get multiple terabits per second. Therefore creating customer-specific custom prefixes within the single bucket and then uploading the daily files into those prefixed locations is the BEST solution for the given constraints.

Incorrect options:

Change the application architecture to create a new S3 bucket for each customer and then upload each customer's files directly under the respective buckets – Creating a new S3 bucket for each new customer is an inefficient way of handling resource availability (S3 buckets need to be globally unique) as some customers may use the service sparingly but the bucket name is locked for them forever. Moreover, this is really not required as we can use S3 prefixes to improve the performance.

Change the application architecture to create a new S3 bucket for each day's data and then upload the daily files directly under that day's bucket – Creating a new S3 bucket for each new day's data is also an inefficient way of handling resource availability (S3 buckets need to be globally unique) as some of the bucket names may not be available for daily data processing. Moreover, this is really not required as we can use S3 prefixes to improve the performance.

Change the application architecture to use EFS instead of Amazon S3 for storing the customers' uploaded files – EFS is a costlier storage option compared to S3, so it is ruled out.

Question 38:

A leading video streaming service delivers billions of hours of content from Amazon S3 to customers around the world. Amazon S3 also serves as the data lake for its big data analytics solution. The data lake has a staging zone where intermediary query results are kept only for 24 hours. These results are also heavily referenced by other parts of the analytics pipeline.

Which of the following is the MOST cost-effective strategy for storing this intermediary query data?

- A. Store the intermediary query results in S3 Intelligent-Tiering storage class
- B. Store the intermediary query results in S3 Standard-Infrequent Access storage class
- C. Store the intermediary query results in S3 One Zone-Infrequent Access storage class
- D. Store the intermediary query results in S3 Standard storage class

Answer: D

Explanation

Correct option:

Store the intermediary query results in S3 Standard storage class

S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics. As there is no minimum storage duration charge and no retrieval fee (remember that intermediary query results are heavily referenced by other parts of the analytics pipeline), this is the MOST cost-effective storage class amongst the given options.

Incorrect options:

Store the intermediary query results in S3 Intelligent-Tiering storage class – The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. The minimum storage duration charge is 30 days, so this option is NOT cost-effective because intermediary query results need to be kept only for 24 hours. Hence this option is not correct.

Store the intermediary query results in S3 Standard-Infrequent Access storage class – S3 Standard-IA is for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA offers high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files. The minimum storage duration charge is 30 days, so this option is NOT cost-effective because intermediary query results need to be kept only for 24 hours. Hence this option is not correct.

Store the intermediary query results in S3 One Zone-Infrequent Access storage class – S3 One Zone-IA is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. The minimum storage duration charge is 30 days, so this option is NOT cost-effective because intermediary query results need to be kept only for 24 hours. Hence this option is not correct.

To summarize again, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA have a minimum storage duration charge of 30 days (so instead of 24 hours, you end up paying for 30 days). S3 Standard-IA and S3 One Zone-IA also have retrieval charges (as the results are heavily referenced by other parts of the analytics pipeline, so the retrieval costs would be pretty high). Therefore, these 3 storage classes are not cost optimal for the given use-case.

Question 39:

A social photo-sharing company uses Amazon S3 to store the images uploaded by the users. These images are kept encrypted in S3 by using AWS-KMS and the company manages its own Customer Master Key (CMK) for encryption. A member of the DevOps team accidentally deleted the CMK a day ago, thereby rendering the user's photo data unrecoverable. You have been contacted by the company to consult them on possible solutions to this crisis.

As a solutions architect, which of the following steps would you recommend to solve this issue?

Options:

- A. Contact AWS support to retrieve the CMK from their backup
- B. The CMK can be recovered by the AWS root account user
- C. The company should issue a notification on its web application informing the users about the loss of their data
- D. As the CMK was deleted a day ago, it must be in the ‘pending deletion’ status and hence you can just cancel the CMK deletion and recover the key

Answer: D

Explanation

Correct option:

As the CMK was deleted a day ago, it must be in the ‘pending deletion’ status and hence you can just cancel the CMK deletion and recover the key

AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2.

Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. Therefore, AWS KMS enforces a waiting period. To delete a CMK in AWS KMS you schedule key deletion. You can set the waiting period from a minimum of 7 days up to a maximum of 30 days. The default waiting period is 30 days. During the waiting period, the CMK status and key state is Pending deletion. To recover the CMK, you can cancel key deletion before the waiting period ends. After the waiting period ends you cannot cancel key deletion, and AWS KMS deletes the CMK.

Incorrect options:

Contact AWS support to retrieve the CMK from their backup

The CMK can be recovered by the AWS root account user

The AWS root account user cannot recover CMK and the AWS support does not have access to CMK via any backups. Both these options just serve as distractors.

The company should issue a notification on its web application informing the users about the loss of their data – This option is not required as the data can be recovered via the cancel key deletion feature.

Question 40:

A company uses Amazon S3 buckets for storing sensitive customer data. The company has defined different retention periods for different objects present in the Amazon S3 buckets, based on the compliance requirements. But, the retention rules do not seem to work as expected.

Which of the following options represent a valid configuration for setting up retention periods for objects in Amazon S3 buckets?

(Select two)

Options:

- A. When you apply a retention period to an object version explicitly, you specify a Retain Until Date for the object version
- B. You cannot place a retention period on an object version through a bucket default setting
- C. When you use bucket default settings, you specify a Retain Until Date for the object version
- D. Different versions of a single object can have different retention modes and periods

E. The bucket default settings will override any explicit retention mode or period you request on an object version

Answer: A & D

Explanation

Correct options:

When you apply a retention period to an object version explicitly, you specify a Retain Until Date for the object version – You can place a retention period on an object version either explicitly or through a bucket default setting. When you apply a retention period to an object version explicitly, you specify a Retain Until Date for the object version. Amazon S3 stores the Retain Until Date setting in the object version’s metadata and protects the object version until the retention period expires.

Different versions of a single object can have different retention modes and periods – Like all other Object Lock settings, retention periods apply to individual object versions. Different versions of a single object can have different retention modes and periods.

For example, suppose that you have an object that is 15 days into a 30-day retention period, and you PUT an object into Amazon S3 with the same name and a 60-day retention period. In this case, your PUT succeeds, and Amazon S3 creates a new version of the object with a 60-day retention period. The older version maintains its original retention period and becomes deletable in 15 days.

Incorrect options:

You cannot place a retention period on an object version through a bucket default setting – You can place a retention period on an object version either explicitly or through a bucket default setting.

When you use bucket default settings, you specify a Retain Until Date for the object version – When you use bucket default settings, you don’t specify a Retain Until Date. Instead, you specify a duration, in either days or years, for which every object version placed in the bucket should be protected.

The bucket default settings will override any explicit retention mode or period you request on an object version – If your request to place an object version in a bucket contains an explicit retention mode and period, those settings override any bucket default settings for that object version.

Question 41:

A data analytics company measures what the consumers watch and what advertising they’re exposed to. This real-time data is ingested into its on-premises data center and subsequently, the daily data feed is compressed into a single file and uploaded on Amazon S3 for backup. The typical compressed file size is around 2 GB.

Which of the following is the fastest way to upload the daily compressed file into S3?

Options:

- A. Upload the compressed file using multipart upload with S3 transfer acceleration
- B. Upload the compressed file in a single operation
- C. Upload the compressed file using multipart upload
- D. FTP the compressed file into an EC2 instance that runs in the same region as the S3 bucket. Then transfer the file from the EC2 instance into the S3 bucket

Answer: A

Explanation

Correct option:

Upload the compressed file using multipart upload with S3 transfer acceleration

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront’s globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

Multipart upload allows you to upload a single object as a set of parts. Each part is a contiguous portion of the object’s data. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. If you’re uploading large objects over a stable high-bandwidth network, use multipart uploading to maximize the use of your available bandwidth by uploading object parts in parallel for multi-threaded performance. If you’re uploading over a spotty network, use multipart uploading to increase resiliency to network errors by avoiding upload restarts.

Incorrect options:

Upload the compressed file in a single operation – In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation. Multipart upload provides improved throughput – you can upload parts in parallel to improve throughput. Therefore, this option is not correct.

Upload the compressed file using multipart upload – Although using multipart upload would certainly speed up the process, combining with S3 transfer acceleration would further improve the transfer speed. Therefore just using multipart upload is not the

correct option.

FTP the compressed file into an EC2 instance that runs in the same region as the S3 bucket. Then transfer the file from the EC2 instance into the S3 bucket – This is a roundabout process of getting the file into S3 and added as a distractor. Although it is technically feasible to follow this process, it would involve a lot of scripting and certainly would not be the fastest way to get the file into S3.

Question 43:

A technology blogger wants to write a review on the comparative pricing for various storage types available on AWS Cloud. The blogger has created a test file of size 1GB with some random data. Next he copies this test file into AWS S3 Standard storage class, provisions an EBS volume (General Purpose SSD (gp2)) with 100GB of provisioned storage and copies the test file into the EBS volume, and lastly copies the test file into an EFS Standard Storage filesystem. At the end of the month, he analyses the bill for costs incurred on the respective storage types for the test file.

What is the correct order of the storage charges incurred for the test file on these three storage types?

Options:

- A. Cost of test file storage on S3 Standard < Cost of test file storage on EBS < Cost of test file storage on EFS
- B. Cost of test file storage on S3 Standard < Cost of test file storage on EFS < Cost of test file storage on EBS
- C. Cost of test file storage on EFS < Cost of test file storage on S3 Standard < Cost of test file storage on EBS
- D. Cost of test file storage on EBS < Cost of test file storage on S3 Standard < Cost of test file storage on EFS

Answer: B

Explanation

Correct option:

Cost of test file storage on S3 Standard < Cost of test file storage on EFS < Cost of test file storage on EBS

With Amazon EFS, you pay only for the resources that you use. The EFS Standard Storage pricing is \$0.30 per GB per month. Therefore the cost for storing the test file on EFS is \$0.30 for the month.

For EBS General Purpose SSD (gp2) volumes, the charges are \$0.10 per GB-month of provisioned storage. Therefore, for a provisioned storage of 100GB for this use-case, the monthly cost on EBS is $\$0.10 \times 100 = \10 . This cost is irrespective of how much storage is actually consumed by the test file.

For S3 Standard storage, the pricing is \$0.023 per GB per month. Therefore, the monthly storage cost on S3 for the test file is \$0.023.

Therefore this is the correct option.

Incorrect options:

Cost of test file storage on S3 Standard < Cost of test file storage on EBS < Cost of test file storage on EFS

Cost of test file storage on EFS < Cost of test file storage on S3 Standard < Cost of test file storage on EBS

Cost of test file storage on EBS < Cost of test file storage on S3 Standard < Cost of test file storage on EFS

Following the computations shown earlier in the explanation, these three options are incorrect.

Question 37:

An IT company provides S3 bucket access to specific users within the same account for completing project specific work. With changing business requirements, cross-account S3 access requests are also growing every month. The company is looking for a solution that can offer user level as well as account-level access permissions for the data stored in S3 buckets.

As a Solutions Architect, which of the following would you suggest as the MOST optimized way of controlling access for this use-case?

- A• Use Security Groups
- B• Use Amazon S3 Bucket Policies
- C• Use Identity and Access Management (IAM) policies
- D• Use Access Control Lists (ACLs)

Answer: B

Explanation

Correct option:

Use Amazon S3 Bucket Policies

Bucket policies in Amazon S3 can be used to add or deny permissions across some or all of the objects within a single bucket. Policies can be attached to users, groups, or Amazon S3 buckets, enabling centralized management of permission. ↑
With bucket policies, you can grant users within your AWS Account or other AWS Accounts access to your Amazon S3 resources.

You can further restrict access to specific resources based on certain conditions. For example, you can restrict access based on

request time (Date Condition), whether the request was sent using SSL (Boolean Conditions), a requester's IP address (IP Address Condition), or based on the requester's client application (String Conditions). To identify these conditions, you use policy keys.

Incorrect options:

Use Identity and Access Management (IAM) policies – AWS IAM enables organizations with many employees to create and manage multiple users under a single AWS account. IAM policies are attached to the users, enabling centralized control of permissions for users under your AWS Account to access buckets or objects. With IAM policies, you can only grant users within your own AWS account permission to access your Amazon S3 resources. So, this is not the right choice for the current requirement.

Use Access Control Lists (ACLs) – Within Amazon S3, you can use ACLs to give read or write access on buckets or objects to groups of users. With ACLs, you can only grant other AWS accounts (not specific users) access to your Amazon S3 resources. So, this is not the right choice for the current requirement.

Use Security Groups – A security group acts as a virtual firewall for EC2 instances to control incoming and outgoing traffic. S3 does not support Security Groups, this option just acts as a distractor.

4. Creation of S3 Bucket

5. S3 Pricing Tiers

6. S3 Security and Encryption

7. S3 Version Control

Question 1:

As a Solutions Architect, you are building an SFA on AWS. This SFA has a business requirement for sales reps to upload sales daily. In addition, those records should be kept for sales reports. Report storage requires durable and highly available storage. Since many sales people use SFA, it is an important requirement to prevent these records from being accidentally deleted due to some kind of operation error.

Choose data protection measures to meet these requirements.

Options:

- A. Use S3 for storage and enable its versioning function
- B. Automatically take snapshots on a regular basis while accumulating data on EBS
- C. Take snapshots automatically on a regular basis while accumulating data in S3
- D. Automatically take snapshots on a regular basis while accumulating data on RDS

Answer: A

Explanation

Option 1 is the correct answer. The S3 standard storage class is best for storing frequently used data. On top of that, you can easily restore previous versions of the object by setting versioning. Versioning is a way to keep multiple variants of an object in the same bucket. You can use versioning to store, retrieve, and restore any version of any object stored in your Amazon S3 bucket. Versioning makes it easy to recover data from unintended user actions and application failures.

Option 2 is incorrect. EBS is less durable than S3. EBS is not suitable for data sharing.

Option 3 is incorrect. S3 does not have snapshot functionality.

Option 4 is incorrect. RDS is a relational database and does not meet the requirements for durable and available storage.

8. S3 Life Cycle Management

9. S3 Lock Policies and Glacier Vault Lock

10. S3 Performance

11. S3 Select and Glacier Select

12. AWS Organizations & Consolidate Billing

13. Sharing S3 Buckets between Accounts

14. Cross Region Replication

15. Transfer Acceleration

Question 1:

A news network uses Amazon S3 to aggregate the raw video footage from its reporting teams across the US. The news network has recently expanded into new geographies in Europe and Asia. The technical teams at the overseas branch offices have reported huge delays in uploading large video files to the destination S3 bucket.

Which of the following are the MOST cost-effective options to improve the file upload speed into S3? (Select two)

Options:

- A. Create multiple site-to-site VPN connections between the AWS Cloud and branch offices in Europe and Asia. Use these VPN connections for faster file uploads into S3
- B. Use AWS Global Accelerator for faster file uploads into the destination S3 bucket
- C. Use Amazon S3 Transfer Acceleration to enable faster file uploads into the destination S3 bucket
- D. Create multiple AWS direct connect connections between the AWS Cloud and branch offices in Europe and Asia. Use the direct connect connections for faster file uploads into S3
- E. Use multipart uploads for faster file uploads into the destination S3 bucket

Answer: C & E

Explanation

Correct options:

Use Amazon S3 Transfer Acceleration to enable faster file uploads into the destination S3 bucket – Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

Use multipart uploads for faster file uploads into the destination S3 bucket – Multipart upload allows you to upload a single object as a set of parts. Each part is a contiguous portion of the object's data. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation. Multipart upload provides improved throughput, therefore it facilitates faster file uploads.

Incorrect options:

Create multiple AWS direct connect connections between the AWS Cloud and branch offices in Europe and Asia. Use the direct connect connections for faster file uploads into S3 – AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Direct connect takes significant time (several months) to be provisioned and is an overkill for the given use-case.

Create multiple site-to-site VPN connections between the AWS Cloud and branch offices in Europe and Asia. Use these VPN connections for faster file uploads into S3 – AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). You can securely extend your data center or branch office network to the cloud with an AWS Site-to-Site VPN connection. A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections are a good solution if you have low to modest bandwidth requirements and can tolerate the inherent variability in Internet-based connectivity. Site-to-site VPN will not help in accelerating the file transfer speeds into S3 for the given use-case.

Use AWS Global Accelerator for faster file uploads into the destination S3 bucket – AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances. AWS Global Accelerator will not help in accelerating the file transfer speeds into S3 for the given use-case.

Question 2:

A junior scientist working with the Deep Space Research Laboratory at NASA is trying to upload a high-resolution image of a nebula into Amazon S3. The image size is approximately 3GB. The junior scientist is using S3 Transfer Acceleration (S3TA) for faster image upload. It turns out that S3TA did not result in an accelerated transfer.

Given this scenario, which of the following is correct regarding the charges for this image transfer?

Options:

- A. The junior scientist only needs to pay S3 transfer charges for the image upload
- B. The junior scientist does not need to pay any transfer charges for the image upload
- C. The junior scientist needs to pay both S3 transfer charges and S3TA transfer charges for the image upload
- D. The junior scientist only needs to pay S3TA transfer charges for the image upload

Answer: B

Explanation

Correct option:

The junior scientist does not need to pay any transfer charges for the image upload

There are no S3 data transfer charges when data is transferred in from the internet. Also with S3TA, you pay only for transfers that are accelerated. Therefore the junior scientist does not need to pay any transfer charges for the image upload because S3TA did not result in an accelerated transfer.

Incorrect options:

The junior scientist only needs to pay S3TA transfer charges for the image upload – Since S3TA did not result in an accelerated transfer, there are no S3TA transfer charges to be paid.

The junior scientist only needs to pay S3 transfer charges for the image upload – There are no S3 data transfer charges when data is transferred in from the internet. So this option is incorrect.

The junior scientist needs to pay both S3 transfer charges and S3TA transfer charges for the image upload – There are no S3 data transfer charges when data is transferred in from the internet. Since S3TA did not result in an accelerated transfer, there are no S3TA transfer charges to be paid.

16. DataSync Overview

Question 1:

An organization has a large amount of data on Windows (SMB) file shares in their on-premises data center. The organization would like to move data into Amazon S3. They would like to automate the migration of data over their AWS Direct Connect link.

Which AWS service can assist them?

Options:

- A. AWS Snowball
- B. AWS DataSync
- C. AWS CloudFormation
- D. AWS Database Migration Service (DMS)

Answer: B

Explanation

AWS DataSync can be used to move large amounts of data online between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS). DataSync eliminates or automatically handles many of these tasks, including scripting copy jobs, scheduling and monitoring transfers, validating data, and optimizing network utilization. The source datastore can be Server Message Block (SMB) file servers.

CORRECT: “AWS DataSync” is the correct answer.

INCORRECT: “AWS Database Migration Service (DMS)” is incorrect. AWS Database Migration Service (DMS) is used for migrating databases, not data on file shares.

INCORRECT: “AWS CloudFormation” is incorrect. AWS CloudFormation can be used for automating infrastructure provisioning. This is not the best use case for CloudFormation as DataSync is designed specifically for this scenario.

INCORRECT: “AWS Snowball” is incorrect. AWS Snowball is a hardware device that is used for migrating data into AWS. The organization plan to use their Direct Connect link for migrating data rather than sending it in via a physical device. Also, Snowball will not automate the migration.

Question 2:

A company runs an application in an on-premises data center that collects environmental data from production machinery. The data consists of JSON files stored on network attached storage (NAS) and around 5 TB of data is collected each day. The company must upload this data to Amazon S3 where it can be processed by an analytics application. The data must be transferred securely.

Which solution offers the MOST reliable and time-efficient data transfer?

Options:

- A. AWS Database Migration Service over the internet
- B. Multiple AWS Snowcone devices
- C. AWS DataSync over AWS Direct Connect
- D. Amazon S3 Transfer Acceleration over the Internet

Answer: C

Explanation

The most reliable and time-efficient solution that keeps the data secure is to use AWS DataSync and synchronize the data from the NAS device directly to Amazon S3. This should take place over an AWS Direct Connect connection to ensure reliability, speed, and security.

AWS DataSync can copy data between Network File System (NFS) shares, Server Message Block (SMB) shares, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Elastic File System (Amazon EFS) file systems, and Amazon FSx for Windows File Server file systems.

CORRECT: “AWS DataSync over AWS Direct Connect” is the correct answer.

INCORRECT: “AWS Database Migration Service over the Internet” is incorrect. DMS is for migrating databases, not files.

INCORRECT: “Amazon S3 Transfer Acceleration over the Internet” is incorrect. The Internet does not offer the reliability, speed or performance that this company requires.

INCORRECT: “Multiple AWS Snowcone devices” is incorrect. This is not a time-efficient approach as it can take time to ship these devices in both directions.

17. CloudFront Overview

Question 1:

You are hosting a web server on AWS with an EC2 instance. Recently, the number of image acquisition requests for applications has increased, and these requests occupy most of the CPU usage, resulting in poor application response performance.

What is the appropriate way to improve the usability of this application?

Options:

- A. Increase EC2 instances by setting the ASG
- B. Install an ELB to enable load balancing
- C. Install CloudFront on the front to handle image processing
- D. Set up Dynamo DB to handle high-speed data processing

Answer: C

Explanation

In order to improve usability due to the increase in image acquisition requests, it is desirable to set up CloudFront instead of Auto Scaling and leave the image distribution to AWS. CloudFront is a high-speed content delivery network (CDN) service that delivers content securely to viewers with low-latency, high-speed forwarding. CloudFront connects directly to AWS's global infrastructure as well as its other AWS services.

Option 1 is incorrect. It is possible to improve the processing on the WEB server side by increasing the number of EC2 instances by setting the Auto Scaling group, but it is recommended first to set CloudFront to improve the content distribution processing of the WEB application.

Option 2 is incorrect. It has nothing to do with load balancing and fast image delivery processing.

Option 4 is incorrect. DynamoDB cannot be used to speed up image distribution. DynamoDB is suitable for managing session data and metadata, and for KVS data processing such as high-speed processing.

Question 2:

Your company operates an image distribution application. The Application is using CloudFront to optimize image delivery, but what happens when the content isn't on the edge location?

Choose an action that CloudFront will take in this situation

Options:

- A. CloudFront will take advantage of another edge location where the content is being stored
- B. CloudFront accesses the origin server to retrieve data and then stores it at the edge location
- C. Displays a 404 error because the data is not found
- D. Stalls requests in CloudFront and waits for the requested data to reach the edge location



Answer: B

Explanation

CloudFront optimizes content delivery by caching data at the edge location closest to your users. If the data doesn't exist at the edge location, CloudFront will retrieve the data from the origin server before delivering it, but from the next request onwards, it will be processed from the cache at the edge location. Therefore, option 2 is the correct answer.

Option 1 is incorrect. There is no way to handle the request from another edge location. CloudFront delivers from the edge closer to the user. Therefore, if CloudFront doesn't have a deliverable cache on the appropriate edge for the user, it will retrieve this data from the origin server.

Option 3 is incorrect. CloudFront doesn't show a 404 error because CloudFront doesn't have the right data on the edge.

If it doesn't have a the appropriate data cache on the right edge location for the user, it goes to the origin server to get this data.

Option 4 is incorrect. CloudFront doesn't stock requests and wait for data to reach the edge location.

Question 3:

As a Solutions Architect, you plan to use Route 53 as your DNS server. As a requirement, in order to speed up image distribution etc., it is necessary to use CloudFront distribution using your company's domain name.

Choose the best method to meet this requirement.

Options:

- A. Create a CNAME record to specify CloudFront delivery
- B. Create a A record and specify CloudFront delivery
- C. Create an ALIAS record to specify CloudFront delivery
- D. Create a NS record and specify CloudFront delivery

Answer: C

Explanation

You can configure CloudFront on Route 53 to associate a domain by creating an ALIAS record and configuring CloudFront. Therefore, option 3 is the correct answer.

Regular Route 53 records use standard DNS records, but you should make use of ALIAS records when configuring AWS resources such as CloudFront. ALIAS records provide Route 53-specific extensions to DNS functionality. Instead of an IP address or domain name, the ALIAS record should be a CloudFront, Elastic Beanstalk environment, ELB, a pointer to an Amazon S3 bucket configured as a static website, or another Route 53 record in the same hosted zone.

Option 1 is incorrect. The CNAME record is used to associate another domain with an existing domain.

Option 2 is incorrect. The A record is used to associate the IPv4 address with a domain.

Option 4 is incorrect. NS records are records that specify an authoritative server for a zone.

Question 4:

A company offers an online product brochure that is delivered from a static website running on Amazon S3. The company's customers are mainly in the United States, Canada, and Europe. The company is looking to cost-effectively reduce the latency for users in these regions.

What is the most cost-effective solution to these requirements?

Options:

- A. Create an Amazon CloudFront distribution and use Lambda@Edge to run the website's data processing closer to the users
- B. Create an Amazon CloudFront distribution that uses origins in U.S, Canada and Europe
- C. Create an Amazon CloudFront distribution and set the price class to use all Edge Locations for best performance
- D. Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Europe.

Options: D

Explanation

With Amazon CloudFront you can set the price class to determine where in the world the content will be cached. One of the price classes is "U.S, Canada and Europe" and this is where the company's users are located. Choosing this price class will result in lower costs and better performance for the company's users.

CORRECT: "Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Europe." is the correct answer.

INCORRECT: "Create an Amazon CloudFront distribution and set the price class to use all Edge Locations for best performance" is incorrect. This will be more expensive as it will cache content in Edge Locations all over the world.

INCORRECT: "Create an Amazon CloudFront distribution that uses origins in U.S, Canada and Europe" is incorrect. ↑ origin can be in one place, there's no need to add origins in different Regions. The price class should be used to limit the caching of the

content to reduce cost.

INCORRECT: “Create an Amazon CloudFront distribution and use Lambda@Edge to run the website’s data processing closer to the users” is incorrect. Lambda@Edge will not assist in this situation as there is no data processing required, the content from the static website must simply be cached at an edge location.

Question 5:

A company runs a dynamic website that is hosted on an on-premises server in the United States. The company is expanding to Europe and is investigating how they can optimize the performance of the website for European users. The website’s backed must remain in the United States. The company requires a solution that can be implemented within a few days.

What should a Solutions Architect recommend?

Options:

- A. Use Amazon CloudFront with Lambda@Edge to direct traffic to an on-premises origin
- B. Use Amazon CloudFront with a custom origin pointing to the on-premises servers
- C. Launch an Amazon EC2 instance in an AWS Region in the United States and migrate the website to it
- D. Migrate the website to Amazon S3. Use cross-Region replication between Regions and a latency-based Route 53 policy

Answer: B

Explanation

A custom origin can point to an on-premises server and CloudFront is able to cache content for dynamic websites. CloudFront can provide performance optimizations for custom origins even if they are running on on-premises servers. These include persistent TCP connections to the origin, SSL enhancements such as Session tickets and OCSP stapling.

Additionally, connections are routed from the nearest Edge Location to the user across the AWS global network. If the on-premises server is connected via a Direct Connect (DX) link this can further improve performance.

CORRECT: “Use Amazon CloudFront with a custom origin pointing to the on-premises servers” is the correct answer.

INCORRECT: “Use Amazon CloudFront with Lambda@Edge to direct traffic to an on-premises origin” is incorrect. Lambda@Edge is not used to direct traffic to on-premises origins.

INCORRECT: “Launch an Amazon EC2 instance in an AWS Region in the United States and migrate the website to it” is incorrect. This would not necessarily improve performance for European users.

INCORRECT: “Migrate the website to Amazon S3. Use cross-Region replication between Regions and a latency-based Route 53 policy” is incorrect. You cannot host dynamic websites on Amazon S3 (static only).

Question 6:

A company delivers content to subscribers distributed globally from an application running on AWS. The application uses a fleet of Amazon EC2 instance in a private subnet behind an Application Load Balancer (ALB). Due to an update in copyright restrictions, it is necessary to block access for specific countries.

What is the EASIEST method to meet this requirement?

Options:

- A. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
- B. Use a Network ACL to block the IP address ranges associated with the specific countries
- C. Modify the ALB security group to deny incoming traffic from blocked countries
- D. Use Amazon CloudFront to serve the application and deny access to blocked countries

Answer: D

Explanation

When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following:

Allow your users to access your content only if they’re in one of the countries on a whitelist of approved countries.

Prevent your users from accessing your content if they’re in one of the countries on a blacklist of banned countries.

For example, if a request comes from a country where, for copyright reasons, you are not authorized to distribute your content, you can use CloudFront geo restriction to block the request.

This is the easiest and most effective way to implement a geographic restriction for the delivery of content.

CORRECT: “Use Amazon CloudFront to serve the application and deny access to blocked countries” is the correct answer.

INCORRECT: “Use a Network ACL to block the IP address ranges associated with the specific countries” is incorrect as this would be extremely difficult to manage.

INCORRECT: “Modify the ALB security group to deny incoming traffic from blocked countries” is incorrect as security groups

cannot block traffic by country.

INCORRECT: “Modify the security group for EC2 instances to deny incoming traffic from blocked countries” is incorrect as security groups cannot block traffic by country.

Question 7:

An organization want to share regular updates about their charitable work using static webpages. The pages are expected to generate a large amount of views from around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

Options:

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

Answer: B

Explanation

Amazon CloudFront can be used to cache the files in edge locations around the world and this will improve the performance of the webpages.

To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:

Using a REST API endpoint as the origin with access restricted by an origin access identity (OAI)

Using a website endpoint as the origin with anonymous (public) access allowed

Using a website endpoint as the origin with access restricted by a Referer header

CORRECT: “Use Amazon CloudFront with the S3 bucket as its origin” is the correct answer.

INCORRECT: “Generate presigned URLs for the files” is incorrect as this is used to restrict access which is not a requirement.

INCORRECT: “Use cross-Region replication to all Regions” is incorrect as this does not provide a mechanism for directing users to the closest copy of the static webpages.

INCORRECT: “Use the geoproximity feature of Amazon Route 53” is incorrect as this does not include a solution for having multiple copies of the data in different geographic locations.

Question 8:

A website runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) which serves as an origin for an Amazon CloudFront distribution. An AWS WAF is being used to protect against SQL injection attacks. A review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

Options:

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

Answer: C

Explanation

A new version of the AWS Web Application Firewall was released in November 2019. With AWS WAF classic you create “IP match conditions”, whereas with AWS WAF (new version) you create “IP set match statements”. Look out for wording on the exam.

The IP match condition / IP set match statement inspects the IP address of a web request’s origin against a set of IP addresses and address ranges. Use this to allow or block web requests based on the IP addresses that the requests originate from.

AWS WAF supports all IPv4 and IPv6 address ranges. An IP set can hold up to 10,000 IP addresses or IP address ranges to check.

CORRECT: “Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address” is the correct answer.

INCORRECT: “Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address” is incorrect as CloudFront does not sit within a subnet so network ACLs do not apply to it.

INCORRECT: “Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address” is incorrect as the source IP addresses of the data in the EC2 instances subnets will be the ELB IP address ↑

INCORRECT: “Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.” is incorrect as you cannot create deny rules with security groups.

Question 9:

CloudFront offers a multi-tier cache in the form of regional edge caches that improve latency. However, there are certain content types that bypass the regional edge cache, and go directly to the origin.

Which of the following content types skip the regional edge cache? (Select two)

Options:

- A. Static content such as style sheets, JavaScript files
- B. E-commerce assets such as product photos
- C. Proxy methods PUT/POST/PATCH/OPTIONS/DELETE go directly to the origin
- D. User-generated videos
- E. Dynamic content, as determined at request time (cache-behavior configured to forward all headers)

Answer: C & E

Explanation

Correct options:

Dynamic content, as determined at request time (cache-behavior configured to forward all headers)

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

CloudFront points of presence (POPs) (edge locations) make sure that popular content can be served quickly to your viewers.

CloudFront also has regional edge caches that bring more of your content closer to your viewers, even when the content is not popular enough to stay at a POP, to help improve performance for that content.

Dynamic content, as determined at request time (cache-behavior configured to forward all headers), does not flow through regional edge caches, but goes directly to the origin. So this option is correct.

Proxy methods PUT/POST/PATCH/OPTIONS/DELETE go directly to the origin

Proxy methods PUT/POST/PATCH/OPTIONS/DELETE go directly to the origin from the POPs and do not proxy through the regional edge caches. So this option is also correct.

Incorrect Options:

E-commerce assets such as product photos

User-generated videos

Static content such as style sheets, JavaScript files

The following type of content flows through the regional edge caches – user-generated content, such as video, photos, or artwork; e-commerce assets such as product photos and videos and static content such as style sheets, JavaScript files. Hence these three options are not correct.

18. CloudFront Signed URL's and Cookies

Question 1:

Your company shares some HR videos stored in an Amazon S3 bucket via CloudFront. You need to restrict access to the private content so users coming from specific IP addresses can access the videos and ensure direct access via the Amazon S3 bucket is not possible.

How can this be achieved?

Options:

- A. Configure CloudFront to require users to access the files using a signed URL, and configure the S3 bucket as a website endpoint
- B. Configure CloudFront to require users to access the files using a signed URL, create an origin access identity (OAI) and restrict access to the files in the Amazon S3 bucket to the OAI
- C. Configure CloudFront to require users to access the files using signed cookies, create an origin access identity (OAI) and instruct users to login with the OAI
- D. Configure CloudFront to require users to access the files using signed cookies, and move the files to an encrypted EBS volume

Answer: B

Explanation

A signed URL includes additional information, for example, an expiration date and time, that gives you more control over access to your content. You can also specify the IP address or range of IP addresses of the users who can access your content.

If you use CloudFront signed URLs (or signed cookies) to limit access to files in your Amazon S3 bucket, you may want to prevent users from directly accessing your S3 files by using Amazon S3 URLs. To achieve this you can create an origin access

identity (OAI), which is a special CloudFront user, and associate the OAI with your distribution.

You can then change the permissions either on your Amazon S3 bucket or on the files in your bucket so that only the origin access identity has read permission (or read and download permission).

CORRECT: “Configure CloudFront to require users to access the files using a signed URL, create an origin access identity (OAI) and restrict access to the files in the Amazon S3 bucket to the OAI” is the correct answer.

INCORRECT: “Configure CloudFront to require users to access the files using signed cookies, create an origin access identity (OAI) and instruct users to login with the OAI” is incorrect. Users cannot login with an OAI.

INCORRECT: “Configure CloudFront to require users to access the files using signed cookies, and move the files to an encrypted EBS volume” is incorrect. You cannot use CloudFront to pull data directly from an EBS volume.

INCORRECT: “Configure CloudFront to require users to access the files using a signed URL, and configure the S3 bucket as a website endpoint” is incorrect. You cannot use CloudFront and an OAI when your S3 bucket is configured as a website endpoint.

19. Snowball

Question 1:

A video analytics organization has been acquired by a leading media company. The analytics organization has 10 independent applications with an on-premises data footprint of about 70TB for each application. The CTO of the media company has set a timeline of two weeks to carry out the data migration from on-premises data center to AWS Cloud and establish connectivity.

Which of the following are the MOST cost-effective options for completing the data transfer and establishing connectivity?

(Select two)

- A. Order 1 Snowmobile to complete the one-time data transfer
- B. Setup AWS direct connect to establish connectivity between the on-premises data center and AWS Cloud
- C. Order 70 Snowball Edge Storage Optimized devices to complete the one-time data transfer
- D. Setup Site-to-Site VPN to establish connectivity between the on-premises data center and AWS Cloud
- E. Order 10 Snowball Edge Storage Optimized devices to complete the one-time data transfer

Answer: D & E

Explanation

Correct options:

Order 10 Snowball Edge Storage Optimized devices to complete the one-time data transfer

Snowball Edge Storage Optimized is the optimal choice if you need to securely and quickly transfer dozens of terabytes to petabytes of data to AWS. It provides up to 80 TB of usable HDD storage, 40 vCPUs, 1 TB of SATA SSD storage, and up to 40 Gb network connectivity to address large scale data transfer and pre-processing use cases.

As each Snowball Edge Storage Optimized device can handle 80TB of data, you can order 10 such devices to take care of the data transfer for all applications.

Exam Alert:

The original Snowball devices were transitioned out of service and Snowball Edge Storage Optimized are now the primary devices used for data transfer. You may see the Snowball device on the exam, just remember that the original Snowball device had 80TB of storage space.

Setup Site-to-Site VPN to establish connectivity between the on-premises data center and AWS Cloud

AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). You can securely extend your data center or branch office network to the cloud with an AWS Site-to-Site VPN connection. A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

Therefore this option is the right fit for the given use-case as the connectivity can be easily established within the given timeframe.

Incorrect options:

Order 1 Snowmobile to complete the one-time data transfer – Each Snowmobile has a total capacity of up to 100 petabytes. To migrate large datasets of 10PB or more in a single location, you should use Snowmobile. For datasets less than 10PB or distributed in multiple locations, you should use Snowball. So Snowmobile is not the right fit for this use-case.

Setup AWS direct connect to establish connectivity between the on-premises data center and AWS Cloud – AWS Direct Connect

lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC. Direct Connect involves significant monetary investment and takes at least a month to set up, therefore it's not the correct fit for this use-case.

Order 70 Snowball Edge Storage Optimized devices to complete the one-time data transfer – As the data-transfer can be completed with just 10 Snowball Edge Storage Optimized devices, there is no need to order 70 devices.

Question 2:

You would like to use Snowball to move on-premises backups into a long term archival tier on AWS. Which solution provides the MOST cost savings?

- Create a Snowball job and target a Glacier Deep Archive Vault
- Create a Snowball job and target an S3 bucket. Create a lifecycle policy to immediately move data to Glacier
- Create a Snowball job and target an S3 bucket. Create a lifecycle policy to immediately move data to Glacier Deep Archive (Correct)
- Create a Snowball job and target a Glacier Vault

Explanation

Correct option:

Create a Snowball job and target an S3 bucket. Create a lifecycle policy to immediately move data to Glacier Deep Archive. AWS Snowball, a part of the AWS Snow Family, is a data migration and edge computing device that comes in two options. Snowball Edge Storage Optimized devices provide both block storage and Amazon S3-compatible object storage, and 40 vCPUs. They are well suited for local storage and large scale data transfer. Snowball Edge Compute Optimized devices provide 52 vCPUs, block and object storage, and an optional GPU for use cases like advanced machine learning and full-motion video analysis in disconnected environments.

Snowball Edge Storage Optimized is the optimal choice if you need to securely and quickly transfer dozens of terabytes to petabytes of data to AWS. It provides up to 80 TB of usable HDD storage, 40 vCPUs, 1 TB of SATA SSD storage, and up to 40 Gb network connectivity to address large scale data transfer and pre-processing use cases.

The original Snowball devices were transitioned out of service and Snowball Edge Storage Optimized are now the primary devices used for data transfer. You may see the Snowball device on the exam, just remember that the original Snowball device had 80TB of storage space.

You can't move data directly from Snowball into Glacier, you need to go through S3 first, and then use a lifecycle policy. So this option is correct.

Incorrect options:

Create a Snowball job and target a Glacier Vault

Create a Snowball job and target a Glacier Deep Archive Vault

Amazon S3 Glacier and S3 Glacier Deep Archive are a secure, durable, and extremely low-cost Amazon S3 cloud storage classes for data archiving and long-term backup. They are designed to deliver 99.99999999% durability and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. Finally, Glacier Deep Archive provides more cost savings than Glacier.

Both these options are incorrect as you can't move data directly from Snowball into a Glacier Vault or a Glacier Deep Archive Vault. You need to go through S3 first and then use a lifecycle policy.

Create a Snowball job and target an S3 bucket. Create a lifecycle policy to immediately move data to Glacier – As Glacier Deep Archive provides more cost savings than Glacier, so you should use Glacier Deep Archive for long term archival for this use-case.

20. Storage Gateway

Question 1: A company wants to host its internal storage on AWS. This storage is required to be connected to an on-premises application server via an iSCSI device. In addition, after the migration is complete, they plan to use the storage on AWS as their primary storage. Choose a configuration method that can meet this requirement.

Options:

- A. Create an S3 bucket and use the S3 connector as an iSCSI device
- B. Create an EBS and use the EBS connector as an iSCSI device
- C. Create a Glacier archive and use Glacier connector as an iSCSI device

D. Use the AWS storage gateway as an iSCSI device**Answer:** D**Explanation**

Option D is the correct answer. Storage gateway cached volumes allow you to use Amazon S3 as your primary data storage while keeping frequently accessed data locally. Volumes cached in an on-premises environment provide low-latency access to frequently accessed data. You can create storage volumes up to 32 TiB in size and attach them from your on-premises application server via an iSCSI device. The cached volume is the method to be selected when using the AWS side as the primary.

Options A, B and C are incorrect. These services do not have the ability to connect to the on-premises side via an iSCSI device.

Question 2:

Your company owns 3TB volume data in its on-premises repository and stores a large number of files there. This repository is increasing in capacity by 500 GB annually and should be used as a single logical volume. As a Solutions Architect, you have decided to extend this repository to S3 storage to avoid local storage capacity constraints. You also want to maintain optimal response times for frequently accessed data. The plan is to use S3 as the primary.

Which of the following AWS Storage Gateway configurations meets this requirement?

Options:

- A. Cached volume that uses snapshots scheduled to move to S3
- B. Storage type that uses snapshots scheduled to move to S3
- C. Cached that utilize snapshots scheduled to move to Glacier
- D. A virtual type library that utilizes snapshots scheduled to move to S3

Answer: A**Explanation**

Cached volumes on the storage gateway allow you to use S3 as your primary data storage while keeping frequently accessed data in your local environment. Therefore, option 1 is the correct answer.

Cached volumes minimize the need to scale your on-premises storage infrastructure. At the same time, applications will continue to have low-latency access to frequently accessed data. You can create up to 32TiB of storage volumes and attach them as iSCSI devices to your on-premises application server. The gateway stores the data in a storage volume created in Amazon S3, which keeps the recently loaded data in the cache of the on-premises storage gateway, and uploads it to buffer storage.

Option 2 is incorrect. Storage type volumes utilize local storage as the primary and asynchronously back up that data to S3. This time the cached volume meets the requirements.

Option 3 is incorrect. It is appropriate to use S3 storage for hybrid configurations with storage gateways. In addition, Glacier is used to save infrequently used files over the medium to long term, so Option 3 is inappropriate for this requirement.

Option 4 is incorrect. The virtual tape library is used for tape-format backups, and option 4 is inappropriate.

Question 3:

A company is investigating methods to reduce the expenses associated with on-premises backup infrastructure. The Solutions Architect wants to reduce costs by eliminating the use of physical backup tapes. It is a requirement that existing backup applications and workflows should continue to function.

What should the Solutions Architect recommend?

Options

- A. Create an Amazon EFS file system and connect the backup applications using the iSCSI protocol
- B. Connect the backup applications to an AWS Storage Gateway using the NFS protocol
- C. Create an Amazon EFS file system and connect the backup applications using the NFS protocol
- D. Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL)

Answer: D**Explanation**

The AWS Storage Gateway Tape Gateway enables you to replace using physical tapes on premises with virtual tapes in AWS without changing existing backup workflows. Tape Gateway emulates physical tape libraries, removes the cost and complexity of managing physical tape infrastructure, and provides more durability than physical tapes.

CORRECT: “Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL)” is the correct answer.

INCORRECT: “Create an Amazon EFS file system and connect the backup applications using the NFS protocol” is correct. The NFS protocol is used by AWS Storage Gateway File Gateways but these do not provide virtual tape functionality to replace the existing backup infrastructure.

INCORRECT: “Create an Amazon EFS file system and connect the backup applications using the iSCSI protocol” is incorrect. The NFS protocol is used by AWS Storage Gateway File Gateways but these do not provide virtual tape functionality that is suitable for replacing the existing backup infrastructure.

INCORRECT: “Connect the backup applications to an AWS Storage Gateway using the NFS protocol” is incorrect. The iSCSI protocol is used by AWS Storage Gateway Volume Gateways but these do not provide virtual tape functionality that is suitable for replacing the existing backup infrastructure.

Question 4:

Storage capacity has become an issue for a company that runs application servers on-premises. The servers are connected to a combination of block storage and NFS storage solutions. The company requires a solution that supports local caching without re-architecting its existing applications.

Which combination of changes can the company make to meet these requirements? (Select TWO.)

Options:

- A. Use AWS Direct Connect and mount an Amazon FSx for Windows File Server using iSCSI
- B. Use Amazon Elastic File System (EFS) volumes to replace the block storage
- C. Use the mount command on servers to mount Amazon S3 buckets using NFS
- D. Use an AWS Storage Gateway volume gateway to replace the block storage
- E. Use an AWS Storage Gateway file gateway to replace the NFS storage

Answer: D & E

Explanation

In this scenario the company should use cloud storage to replace the existing storage solutions that are running out of capacity. The on-premises servers mount the existing storage using block protocols (iSCSI) and file protocols (NFS). As there is a requirement to avoid re-architecting existing applications these protocols must be used in the revised solution.

The AWS Storage Gateway volume gateway should be used to replace the block-based storage systems as it is mounted over iSCSI and the file gateway should be used to replace the NFS file systems as it uses NFS.

CORRECT: “Use an AWS Storage Gateway file gateway to replace the NFS storage” is a correct answer.

CORRECT: “Use an AWS Storage Gateway volume gateway to replace the block storage” is a correct answer.

INCORRECT: “Use the mount command on servers to mount Amazon S3 buckets using NFS” is incorrect. You cannot mount S3 buckets using NFS as it is an object-based storage system (not file-based) and uses an HTTP REST API.

INCORRECT: “Use AWS Direct Connect and mount an Amazon FSx for Windows File Server using iSCSI” is incorrect. You cannot mount FSx for Windows File Server file systems using iSCSI, you must use SMB.

INCORRECT: “Use Amazon Elastic File System (EFS) volumes to replace the block storage” is incorrect. You cannot use EFS to replace block storage as it uses NFS rather than iSCSI.

Question 5:

A company runs an application in a factory that has a small rack of physical compute resources. The application stores data on a network attached storage (NAS) device using the NFS protocol. The company requires a daily offsite backup of the application data.

Which solution can a Solutions Architect recommend to meet this requirement?

Options:

- A. Create an IPsec VPN to AWS and configure the application to mount the Amazon EFS file system. Run a copy job to backup the data to EFS
- B. Use an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3
- C. Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3
- D. Use an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3

Answer: C

Explanation

The AWS Storage Gateway Hardware Appliance is a physical, standalone, validated server configuration for on-premises deployments. It comes pre-loaded with Storage Gateway software, and provides all the required CPU, memory, network, and SSD cache resources for creating and configuring File Gateway, Volume Gateway, or Tape Gateway.

A file gateway is the correct type of appliance to use for this use case as it is suitable for mounting via the NFS and SMB protocols.

CORRECT: “Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Am: ↑ 53” is the correct answer.

INCORRECT: “Use an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3” is incorrect. Volume gateways are used for block-based storage and this solution requires NFS (file-based storage).

INCORRECT: “Use an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3” is incorrect. Volume gateways are used for block-based storage and this solution requires NFS (file-based storage).

INCORRECT: “Create an IPSec VPN to AWS and configure the application to mount the Amazon EFS file system. Run a copy job to backup the data to EFS” is incorrect. It would be better to use a Storage Gateway which will automatically take care of synchronizing a copy of the data to AWS.

Question 6:

As part of a pilot program, a biotechnology company wants to integrate data files from its on-premises analytical application with AWS Cloud via an NFS interface.

Which of the following AWS service is the MOST efficient solution for the given use-case?

Options:

- A. AWS Site-to-Site VPN
- B. AWS Storage Gateway – Volume Gateway
- C. AWS Storage Gateway – Tape Gateway
- D. AWS Storage Gateway – File Gateway

Answer: D

Explanation

Correct option:

AWS Storage Gateway – File Gateway

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. The service provides three different types of gateways – Tape Gateway, File Gateway, and Volume Gateway – that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access.

AWS Storage Gateway’s file interface, or file gateway, offers you a seamless way to connect to the cloud in order to store application data files and backup images as durable objects on Amazon S3 cloud storage. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching. As the company wants to integrate data files from its analytical instruments into AWS via an NFS interface, therefore AWS Storage Gateway – File Gateway is the correct answer.

Incorrect options:

AWS Storage Gateway – Volume Gateway – You can configure the AWS Storage Gateway service as a Volume Gateway to present cloud-based iSCSI block storage volumes to your on-premises applications. Volume Gateway does not support NFS interface, so this option is not correct.

AWS Storage Gateway – Tape Gateway – AWS Storage Gateway – Tape Gateway allows moving tape backups to the cloud. Tape Gateway does not support NFS interface, so this option is not correct.

AWS Site-to-Site VPN – AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). You can securely extend your data center or branch office network to the cloud with an AWS Site-to-Site VPN (Site-to-Site VPN) connection. It uses internet protocol security (IPSec) communications to create encrypted VPN tunnels between two locations. You cannot use AWS Site-to-Site VPN to integrate data files via the NFS interface, so this option is not correct.

21. Athena versus Macie

22. EC2

Question 1:

As a system operator for your company, you manage a set of web servers hosted on EC2 instances with public IP addresses. These IP addresses are associated with specific domain names. Yesterday, the servers were shut down for emergency maintenance. When the servers were started-up again, the website couldn’t be displayed on the internet.

Choose an option that may be the root cause of this issue.

Options:

- A. It is necessary to reconfigure traffic on Route53 after restarting the EC2 instance

- B. Elastic IP was not configured on EC2 instance
- C. ELB health check failed for EC2 instance
- D. Elastic IP is not set for the IP address of the subnet

Answer: B

Explanation

By default, the EC2 instance's public IP address is released after the instance is stopped. As a result, the previous IP address that was mapped to the domain name becomes invalid and you cannot access it. By setting an Elastic IP for the EC2 instance, the IP address will be maintained even after the EC2 instance is restarted, and the domain name corresponding to the IP address can be used continuously. Therefore, option 2 is the correct answer.

Option 1 is incorrect. The overall correct solution is to prevent the IP address from changing at all. With this issue now made (loss of IP address), Route53 setting changes will be required by this is simply a follow-up response. It is not needed if the initial mistake was not made.

Option 3 is incorrect. If you get an ELB health check error on your EC2 instance, it should show an anomaly even before the reboot. This is not a reboot related problem.

Option 4 is incorrect. The IP address of the subnet will not be affected by the reboot.

Question 2:

Your company has told you the requirements for building a database using AWS. This company is required to manage the database environment in-house. As a Solutions Architect, you need to choose the best AWS service from your database requirements.

Select a database construction method that meets this requirement.

Options:

- A. Build a DB using RDS
- B. Build a DB using DynamoDB
- C. Build a DB using Aurora
- D. Build a DB using EC2 instances

Answer: D

Explanation

In order to manage the database environment in-house, it is necessary to completely control the underlying database instance by building a DB using EC2 instances. Therefore, option 4 is the correct answer.

Options 1, 2 and 3 are incorrect. Since other RDS / DynamoDB / Aurora are managed services, the infrastructure environment that configures the database cannot be managed in-house.

Question 3:

The solo founder at a tech startup has just created a brand new AWS account. The founder has provisioned an EC2 instance 1A which is running in region A. Later, he takes a snapshot of the instance 1A and then creates a new AMI in region A from this snapshot. This AMI is then copied into another region B. The founder provisions an instance 1B in region B using this new AMI in region B.

At this point in time, what entities exist in region B?

Options:

- A. 1 EC2 instance and 1 snapshot exist in region B
- B. 1 EC2 instance, 1 AMI and 1 snapshot exist in region B
- C. 1 EC2 instance and 1 AMI exist in region B
- D. 1 EC2 instance and 2 AMIs exist in region B

Answer: B

Explanation

Correct option:

1 EC2 instance, 1 AMI and 1 snapshot exist in region B

An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. When the new AMI is copied from region A into region B, it automatically creates a snapshot in region B because AMIs are based on the underlying snapshots. Further, an instance is created from this AMI in region B. Hence, we have 1 EC2 instance, 1 AMI and 1 snapshot in region B.

Incorrect options:

1 EC2 instance and 1 AMI exist in region B

1 EC2 instance and 2 AMIs exist in region B

1 EC2 instance and 1 snapshot exist in region B

As mentioned earlier in the explanation, when the new AMI is copied from region A into region B, it also creates a snapshot in region B because AMIs are based on the underlying snapshots. In addition, an instance is created from this AMI in region B. So, we have 1 EC2 instance, 1 AMI and 1 snapshot in region B. Hence all three options are incorrect.

Question 04:

A software engineering intern at an e-commerce company is documenting the process flow to provision EC2 instances via the Amazon EC2 API. These instances are to be used for an internal application that processes HR payroll data. He wants to highlight those volume types that cannot be used as a boot volume.

Can you help the intern by identifying those storage volume types that CANNOT be used as boot volumes while creating the instances? (Select two)

Options:

A. Throughput Optimized HDD (st1)

B. Cold HDD (sc1)

C. General Purpose SSD (gp2)

D. Provisioned IOPS SSD (io1)

E. Instance Store

Answer: A & B

Explanation

Correct options:

Throughput Optimized HDD (st1)

Cold HDD (sc1)

The EBS volume types fall into two categories:

SSD-backed volumes optimized for transactional workloads involving frequent read/write operations with small I/O size, where the dominant performance attribute is IOPS.

HDD-backed volumes optimized for large streaming workloads where throughput (measured in MiB/s) is a better performance measure than IOPS.

Throughput Optimized HDD (st1) and Cold HDD (sc1) volume types CANNOT be used as a boot volume, so these two options are correct.

Incorrect options:

General Purpose SSD (gp2)

Provisioned IOPS SSD (io1)

Instance Store

General Purpose SSD (gp2), Provisioned IOPS SSD (io1), and Instance Store can be used as a boot volume.

Question 9: Skipped

An application is currently hosted on four EC2 instances (behind Application Load Balancer) deployed in a single Availability Zone (AZ). To maintain an acceptable level of end-user experience, the application needs at least 4 instances to be always available.

As a solutions architect, which of the following would you recommend so that the application achieves high availability with MINIMUM cost?

- Deploy the instances in one Availability Zones. Launch two instances in the Availability Zone
- Deploy the instances in two Availability Zones. Launch two instances in each Availability Zone
- Deploy the instances in three Availability Zones. Launch two instances in each Availability Zone(Correct)
- Deploy the instances in two Availability Zones. Launch four instances in each Availability Zone

Explanation

Correct option:

Deploy the instances in three Availability Zones. Launch two instances in each Availability Zone

The correct option is to deploy the instances in three Availability Zones and launch two instances in each Availability Zone. Even if one of the AZs goes out of service, still we shall have 4 instances available and the application can maintain an acceptable level of end-user experience. Therefore, we can achieve high availability with just 6 instances in this case.

Incorrect options:

Deploy the instances in two Availability Zones. Launch two instances in each Availability Zone – When we launch two instances in two AZs, we run the risk of falling below the minimum acceptable threshold of 4 instances if one of the AZs fails. So this option is ruled out.

Deploy the instances in two Availability Zones. Launch four instances in each Availability Zone – When we launch four instances in two AZs, we have to bear costs for 8 instances which is NOT cost-optimal. So this option is ruled out.

Deploy the instances in one Availability Zones. Launch two instances in the Availability Zone – We can't have just two instances in a single AZ as that is below the minimum acceptable threshold of 4 instances.

Question 25:

An application runs big data workloads on EC2 instances. The application needs at least 20 instances to maintain a minimum acceptable performance threshold and the application needs 300 instances to handle spikes in the workload. Based on historical workloads processed by the application, it needs 80 instances 80% of the time.

As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution so that it can meet the workload demand in a steady state?

- A• Purchase 80 on-demand instances. Use Auto Scaling Group to provision the remaining instances as spot instances per the workload demand
- B• Purchase 80 spot instances. Use Auto Scaling Group to provision the remaining instances as on-demand instances per the workload demand
- C• Purchase 80 on-demand instances. Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with launch template to provision the mix of on-demand and spot instances)
- D• Purchase 80 reserved instances. Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with launch template to provision the mix of on-demand and spot instances)

Answer: D

Explanation

Correct option:

Purchase 80 reserved instances. Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with launch template to provision the mix of on-demand and spot instances)

As the steady-state workload demand is 80 instances, we can save on costs by purchasing 80 reserved instances. Based on additional workload demand, we can specify a mix of on-demand and spot instances using Application Load Balancer with a launch template to provision the mix of on-demand and spot instances.

Incorrect options:

Purchase 80 on-demand instances. Use Auto Scaling Group to provision the remaining instances as spot instances per the workload demand – Provisioning 80 on-demand instances would end up costlier than the option where we provision 80 reserved instances. So this option is ruled out.

Purchase 80 on-demand instances. Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with launch template to provision the mix of on-demand and spot instances) – Provisioning 80 on-demand instances would end up costlier than the option where we provision 80 reserved instances. So this option is ruled out.

Purchase 80 spot instances. Use Auto Scaling Group to provision the remaining instances as on-demand instances per the workload demand – The option to purchase 80 spot instances is incorrect, as there is no guarantee regarding the availability of the spot instances, which means we may not even meet the steady-state workload.

Question 28:

An engineering team wants to examine the feasibility of the user data feature of Amazon EC2 for an upcoming project.

Which of the following are true about the EC2 user data configuration? (Select two)

- A• By default, user data is executed every time an EC2 instance is re-started
- B• By default, user data runs only during the boot cycle when you first launch an instance
- C• By default, scripts entered as user data do not have root user privileges for executing
- D• When an instance is running, you can update user data by using root user credentials
- E• By default, scripts entered as user data are executed with root user privileges

Answer: B & E

Explanation

Correct options:

User Data is generally used to perform common automated configuration tasks and even run scripts after the instance starts. When you launch an instance in Amazon EC2, you can pass two types of user data – shell scripts and cloud-init directives. You can also pass this data into the launch wizard as plain text or as a file.

By default, scripts entered as user data are executed with root user privileges – Scripts entered as user data are executed as the root user, hence do not need the sudo command in the script. Any files you create will be owned by root; if you need non-root

users to have file access, you should modify the permissions accordingly in the script.

By default, user data runs only during the boot cycle when you first launch an instance – By default, user data scripts and cloud-init directives run only during the boot cycle when you first launch an instance. You can update your configuration to ensure that your user data scripts and cloud-init directives run every time you restart your instance.

Incorrect options:

By default, user data is executed every time an EC2 instance is re-started – As discussed above, this is not a default configuration of the system. But, can be achieved by explicitly configuring the instance.

When an instance is running, you can update user data by using root user credentials – You can't change the user data if the instance is running (even by using root user credentials), but you can view it.

By default, scripts entered as user data do not have root user privileges for executing – Scripts entered as user data are executed as the root user, hence do not need the sudo command in the script.

23. Security Groups

Question 1:

As a Solutions Architect, you plan to build a web application consisting of a web server and a database server. The web server and database server will be hosted on different EC2 instances, each located on a different subnet. The database server should only allow traffic from the web server.

Please choose a response to meet this requirement.

Options:

- A. Control traffic with VPC endpoints
- B. Control traffic with security groups
- C. Control traffic with NACLs
- D. Allow access from the web server to the DB server with the IAM role

Answer: B

Explanation

Security groups are a good way to control traffic between instances. You can control traffic from a particular EC2 instance by specifying the IP address of the EC2 instance within a security group. Therefore, option 2 is the correct answer.

Option 1 is incorrect. A VPC endpoint is a mechanism that allows AWS resources inside a VPC to access AWS services outside the VPC, and is not used to control traffic.

Option 3 is incorrect. Network ACLs can also control traffic, but this applies only to traffic between a subnet and the internet, not subnet to subnet communication. The security group controls the traffic on his EC2 and other instances. Therefore, security groups are the suitable solution for controlling traffic between EC2 instances.

Option 4 is incorrect. Instead of controlling the traffic from the web server to the database server with the IAM role, the security group is used for control. RDS can perform access authentication by using the database authentication function that uses the IAM role.

Question 2:

Your company has set up security groups on multiple EC2 instances. As an operations personnel, you have decided to change the access settings to your EC2 instance. You have set the security group rules to allow inbound traffic on a new port and with new protocol. You then used this security group to launch a new EC2 instance.

How will the security group settings be reflected?

Options:

- A. Security group changes are immediately reflected in all EC2 instances
- B. It takes time for the SG to be reflected in the EC2 instances for which the security group has been set
- C. Unlike the reflection in the existing EC2 instance, the security group is reflected in the new EC2 instance immediately
- D. It takes a few minutes for the security group to be reflected on all EC2 instances

Answer: A

Explanation

Security group changes and new settings are immediately reflected in all EC2 instances.

Therefore, option 1 is the correct answer.

All other options are incorrect.



Question 3:

- A company has moved its business critical data to Amazon EFS file system which will be accessed by multiple EC2 instances. As an AWS Certified Solutions Architect Associate, which of the following would you recommend to exercise access control such that only the permitted EC2 instances can read from the EFS file system? (Select three)
- A. Attach an IAM policy to your file system to control clients who can mount your file system with the required permissions
 - B. Use VPC security groups to control the network traffic to and from your file system
 - C. Use Network ACLs to control the network traffic to and from your Amazon EC2 instance
 - D. Set up the IAM policy root credentials to control and configure the clients accessing the EFS file system
 - E. Use EFS Access Points to manage application access
 - F. Use Amazon GuardDuty to curb unwanted access to EFS file system

Answer: A, B & E

Explanation**Correct options:**

Use VPC security groups to control the network traffic to and from your file system

Attach an IAM policy to your file system to control clients who can mount your file system with the required permissions

Use EFS Access Points to manage application access

You control which EC2 instances can access your EFS file system by using VPC security group rules and AWS Identity and Access Management (IAM) policies. Use VPC security groups to control the network traffic to and from your file system. Attach an IAM policy to your file system to control which clients can mount your file system and with what permissions, and use EFS Access Points to manage application access. Control access to files and directories with POSIX-compliant user and group-level permissions.

Files and directories in an Amazon EFS file system support standard Unix-style read, write, and execute permissions based on the user ID and group IDs. When an NFS client mounts an EFS file system without using an access point, the user ID and group ID provided by the client is trusted. You can use EFS access points to override user ID and group IDs used by the NFS client. When users attempt to access files and directories, Amazon EFS checks their user IDs and group IDs to verify that each user has permission to access the objects

Incorrect options:

Use Network ACLs to control the network traffic to and from your Amazon EC2 instance - Network ACLs operate at the subnet level and not at the instance level.

Set up the IAM policy root credentials to control and configure the clients accessing the EFS file system - There is no such thing as an IAM policy root credentials and this statement has been added as a distractor.

Use Amazon GuardDuty to curb unwanted access to EFS file system - Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. It cannot be used for access control to the EFS file system.

Question 04:

The engineering team at an e-commerce company is working on cost optimizations for EC2 instances. The team wants to manage the workload using a mix of on-demand and spot instances across multiple instance types. They would like to create an Auto Scaling group with a mix of these instances.

Which of the following options would allow the engineering team to provision the instances for this use-case?

- You can only use a launch configuration to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost
- You can use a launch configuration or a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost
- You can neither use a launch configuration nor a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost
- You can only use a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost (Correct)

Explanation**Correct option:**

You can only use a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost

A launch template is similar to a launch configuration, in that it specifies instance configuration information such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, security groups, and the other parameters that you use to launch

EC2 instances. Also, defining a launch template instead of a launch configuration allows you to have multiple versions of a template.

With launch templates, you can provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost. Hence this is the correct option.

Incorrect options:

You can only use a launch configuration to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost

You can use a launch configuration or a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost

A launch configuration is an instance configuration template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping.

You cannot use a launch configuration to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances. Therefore both these options are incorrect.

You can neither use a launch configuration nor a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost – You can use a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances. So this option is incorrect.

Question 13: Skipped

A developer has configured inbound traffic for the relevant ports in both the Security Group of the EC2 instance as well as the Network Access Control List (NACL) of the subnet for the EC2 instance. The developer is, however, unable to connect to the service running on the Amazon EC2 instance.

As a solutions architect, how will you fix this issue?

- IAM Role defined in the Security Group is different from the IAM Role that is given access in the Network ACLs
- Security Groups are stateful, so allowing inbound traffic to the necessary ports enables the connection. Network ACLs are stateless, so you must allow both inbound and outbound traffic (Correct)
- Rules associated with Network ACLs should never be modified from command line. An attempt to modify rules from command line blocks the rule and results in an erratic behavior
- Network ACLs are stateful, so allowing inbound traffic to the necessary ports enables the connection. Security Groups are stateless, so you must allow both inbound and outbound traffic

Explanation

Correct option:

Security Groups are stateful, so allowing inbound traffic to the necessary ports enables the connection. Network ACLs are stateless, so you must allow both inbound and outbound traffic – Security groups are stateful, so allowing inbound traffic to the necessary ports enables the connection. Network ACLs are stateless, so you must allow both inbound and outbound traffic.

To enable the connection to a service running on an instance, the associated network ACL must allow both inbound traffic on the port that the service is listening on as well as allow outbound traffic from ephemeral ports. When a client connects to a server, a random port from the ephemeral port range (1024-65535) becomes the client's source port.

The designated ephemeral port then becomes the destination port for return traffic from the service, so outbound traffic from the ephemeral port must be allowed in the network ACL.

By default, network ACLs allow all inbound and outbound traffic. If your network ACL is more restrictive, then you need to explicitly allow traffic from the ephemeral port range.

If you accept traffic from the internet, then you also must establish a route through an internet gateway. If you accept traffic over VPN or AWS Direct Connect, then you must establish a route through a virtual private gateway.

Incorrect options:

Network ACLs are stateful, so allowing inbound traffic to the necessary ports enables the connection. Security Groups are stateless, so you must allow both inbound and outbound traffic – This is incorrect as already discussed.

IAM Role defined in the Security Group is different from the IAM Role that is given access in the Network ACLs – This is a made-up option and just added as a distractor.

Rules associated with Network ACLs should never be modified from command line. An attempt to modify rules from command line blocks the rule and results in an erratic behavior – This option is a distractor. AWS does not support modifying network ACLs from the command line tool.

24. EBS

Question 1:

A company runs an application on an Amazon EC2 instance that requires 250 GB of storage space. The application is not used often and has small spikes in usage on weekday mornings and afternoons. The disk I/O can vary with peaks hitting a maximum of 3,000 IOPS. A Solutions Architect must recommend the most cost-effective storage solution that delivers the performance required.

Which solution should the solutions architect recommend?

Options:

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

Answer: D

Explanation

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time.

Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

In this configuration the volume will provide a baseline performance of 750 IOPS but will always be able to burst to the required 3,000 IOPS during periods of increased traffic.

CORRECT: “Amazon EBS General Purpose SSD (gp2)” is the correct answer.

INCORRECT: “Amazon EBS Provisioned IOPS SSD (io1)” is incorrect. The io1 volume type will be more expensive and is not necessary for the performance levels required.

INCORRECT: “Amazon EBS Cold HDD (sc1)” is incorrect. The sc1 volume type is not going to deliver the performance requirements as it cannot burst to 3,000 IOPS.

INCORRECT: “Amazon EBS Throughput Optimized HDD (st1)” is incorrect. The st1 volume type is not going to deliver the performance requirements as it cannot burst to 3,000 IOPS.

Question 2:

A persistent database must be migrated from an on-premises server to an Amazon EC2 instances. The database requires 64,000 IOPS and, if possible, should be stored on a single Amazon EBS volume.

Which solution should a Solutions Architect recommend?

Options:

- A. Create an Amazon EC2 instance with four Amazon EBS General Purpose SSD (gp2) volumes attached. Max out the IOPS on each volume and use a RAID 0 stripe set
- B. Create a Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Provision 64,000 IOPS for the volume
- C. Create an Amazon EC2 instance with two Amazon EBS Provisioned IOPS SSD (io1) volumes attached. Provision 32,000 IOPS per volume and create a logical volume using the OS that aggregates the capacity
- D. Use an instance from the I3 I/O optimized family and leverage instance store storage to achieve the IOPS requirement

Answer: B

Explanation

Amazon EC2 Nitro-based systems are not required for this solution but do offer advantages in performance that will help to maximize the usage of the EBS volume. For the data storage volume an io1 volume can support up to 64,000 IOPS so a single volume with sufficient capacity (50 IOPS per GiB) can be delivered the requirements.

CORRECT: “Create a Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Provision 64,000 IOPS for the volume” is the correct answer.

INCORRECT: “Use an instance from the I3 I/O optimized family and leverage instance store storage to achieve the IOPS requirement” is incorrect.

INCORRECT: “Create an Amazon EC2 instance with four Amazon EBS General Purpose SSD (gp2) volumes attached ↑ max out the IOPS on each volume and use a RAID 0 stripe set” is incorrect. This is not a good use case for gp2 volumes. It is much better to use io1 which also meets the requirement of having a single volume with 64,000 IOPS.

INCORRECT: “Create an Amazon EC2 instance with two Amazon EBS Provisioned IOPS SSD (i01) volumes attached. Provision 32,000 IOPS per volume and create a logical volume using the OS that aggregates the capacity” is incorrect. There is no need to create two volumes and aggregate capacity through the OS, the Solutions Architect can simply create a single volume with 64,000 IOPS.

Question 3:

A company plans to make an Amazon EC2 Linux instance unavailable outside of business hours to save costs. The instance is backed by an Amazon EBS volume. There is a requirement that the contents of the instance’s memory must be preserved when it is made unavailable.

How can a solutions architect meet these requirements?

- A. Terminate the instance outside business hours. Recover the instance again when required
- B. Stop the instance outside business hours. Start the instance again when required
- C. Hibernate the instance outside business hours. Start the instance again when required
- D. Use Auto Scaling to scale down the instance outside of business hours. Scale up the instance when required.

Answer: C

Explanation

When you hibernate an instance, Amazon EC2 signals the operating system to perform hibernation (suspend-to-disk). Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. Amazon EC2 persists the instance’s EBS root volume and any attached EBS data volumes. When you start your instance:

- The EBS root volume is restored to its previous state
- The RAM contents are reloaded
- The processes that were previously running on the instance are resumed
- Previously attached data volumes are reattached and the instance retains its instance ID

CORRECT: “Hibernate the instance outside business hours. Start the instance again when required” is the correct answer.

INCORRECT: “Stop the instance outside business hours. Start the instance again when required” is incorrect. When an instance is stopped the operating system is shut down and the contents of memory will be lost.

INCORRECT: “Use Auto Scaling to scale down the instance outside of business hours. Scale out the instance when required” is incorrect. Auto Scaling scales does not scale up and down, it scales in by terminating instances and out by launching instances. When scaling out new instances are launched and no state will be available from terminated instances.

INCORRECT: “Terminate the instance outside business hours. Recover the instance again when required” is incorrect. You cannot recover terminated instances, you can recover instances that have become impaired in some circumstances.

25. Volumes & Snapshots

Question 1:

One company uses EC2 instances with EBS volumes as server infrastructure. The company’s system operations policy states that all data must be backed up efficiently.

Choose the cost-optimal EBS volume backup method.

Options:

- A. Set up periodic snapshot acquisition for EBS
- B. Use EBS volume encryption
- C. Use the EC2 instance store
- D. Configure mirroring for two EBS volumes

Answer: A

Explanation

Option 1 is the correct answer. EBS snapshots allow you to back up data on Amazon EBS volumes to Amazon S3. Snapshots are incremental backups. That is, after the first snapshot, only the blocks on the device that have changed since the last time are saved. This minimizes the time required to take a snapshot and saves storage costs.

Option 2 is incorrect. EBS volume encryption is used for data protection and is not used for data backup.

Option 3 is incorrect. The EC2 instance store is used to store temporary data and is not relevant to this requirement.

Option 4 is incorrect. It is inefficient to have a mirroring configuration for the entire EBS volume. The mirroring configuration is not for backup, but for the redundancy of EBS volumes, allowing you to continue processing on another disk if one volume fails.

Question 2:

A company wants some EBS volumes with maximum possible Provisioned IOPS (PIOPS) to support high-performance database workloads on EC2 instances. The company also wants some EBS volumes that can be attached to multiple EC2 instances in the same Availability Zone.

As an AWS Certified Solutions Architect Associate, which of the following options would you identify as correct for the given requirements? (Select two)

Options:

- A. Use io1/io2 volumes to enable Multi-Attach on Nitro-based EC2 instances
- B. Use io2 volumes on Nitro-based EC2 instances to achieve a maximum Provisioned IOPS of 256,000
- C. Use gp2 volumes to enable Multi-Attach on Nitro-based EC2 instances
- D. Use gp3 volumes on Nitro-based EC2 instances to achieve a maximum Provisioned IOPS of 256,000
- E. Use io2 Block Express volumes on Nitro-based EC2 instances to achieve a maximum Provisioned IOPS of 256,000

Answer: A & E

Explanation

Correct options:

Use io2 Block Express volumes on Nitro-based EC2 instances to achieve a maximum Provisioned IOPS of 256,000

EBS io2 Block Express is the next generation of Amazon EBS storage server architecture. It has been built for the purpose of meeting the performance requirements of the most demanding I/O intensive applications that run on Nitro-based Amazon EC2 instances. With io2 Block Express volumes, you can provision volumes with Provisioned IOPS (PIOPS) up to 256,000, with an IOPS:GiB ratio of 1,000:1

Use io1/io2 volumes to enable Multi-Attach on Nitro-based EC2 instances

Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances that are in the same Availability Zone. You can attach multiple Multi-Attach enabled volumes to an instance or set of instances. Each instance to which the volume is attached has full read and write permission to the shared volume. Multi-Attach makes it easier for you to achieve higher application availability in clustered Linux applications that manage concurrent write operations.

Incorrect options:

Use io2 volumes on Nitro-based EC2 instances to achieve a maximum Provisioned IOPS of 256,000 For io2, Provisioned IOPS SSD volumes can range in size from 4 GiB to 16 TiB and you can provision from 100 IOPS up to 64,000 IOPS per volume. You can achieve only up to 64,000 IOPS on the instances built on the Nitro System.

Use gp3 volumes on Nitro-based EC2 instances to achieve a maximum Provisioned IOPS of 256,000 – gp3 volumes cannot be used with Nitro-based EC2 instances. In addition, gp3 volumes support a maximum PIOPS of 16,000.

Use gp2 volumes to enable Multi-Attach on Nitro-based EC2 instances – gp2 volumes are not supported for Multi-Attach.

Question 8: Skipped

A junior DevOps engineer wants to change the default configuration for EBS volume termination. By default, the root volume of an EC2 instance for an EBS-backed AMI is deleted when the instance terminates.

Which option below helps change this default behavior to ensure that the volume persists even after the instance terminates?

- Set the TerminateOnDelete attribute to false
- Set the DeleteOnTermination attribute to false (Correct)
- Set the TerminateOnDelete attribute to true
- Set the DeleteOnTermination attribute to true

Explanation

Correct option:

Set the DeleteOnTermination attribute to false

An EC2 instance can be launched from either an instance store-backed AMI or an Amazon EBS-backed AMI. Instances that use Amazon EBS for the root device automatically have an Amazon EBS volume attached. By default, the root volume for an AMI backed by Amazon EBS is deleted when the instance terminates. The default behavior can be changed to ensure that the volume persists after the instance terminates. To change the default behavior, set the DeleteOnTermination attribute to false using a block device mapping.

Incorrect options:

Set the TerminateOnDelete attribute to true

Set the TerminateOnDelete attribute to false

Both these options are incorrect as there is no such attribute as TerminateOnDelete. These options have been added as

distractors.

Set the DeleteOnTermination attribute to true – If you set the DeleteOnTermination attribute to true, then the root volume for an AMI backed by Amazon EBS would be deleted when the instance terminates. Therefore, this option is incorrect.

26. AMI Types (EBS vs Instance Store)

Question 1:

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO.)

Options:

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

Answer: A & E

Explanation

You can copy an Amazon Machine Image (AMI) within or across AWS Regions using the AWS Management Console, the AWS Command Line Interface or SDKs, or the Amazon EC2 API, all of which support the CopyImage action.

Using the copied AMI the solutions architect would then be able to launch an instance from the same EBS volume in the second Region.

Note: the AMIs are stored on Amazon S3, however you cannot view them in the S3 management console or work with them programmatically using the S3 API.

CORRECT: “Copy an Amazon Machine Image (AMI) of an EC2 instance and specify the second Region for the destination” is a correct answer.

CORRECT: “Launch a new EC2 instance from an Amazon Machine Image (AMI) in the second Region” is also a correct answer.

INCORRECT: “Detach a volume on an EC2 instance and copy it to an Amazon S3 bucket in the second Region” is incorrect. You cannot copy EBS volumes directly from EBS to Amazon S3.

INCORRECT: “Launch a new EC2 instance in the second Region and copy a volume from Amazon S3 to the new instance” is incorrect. You cannot create an EBS volume directly from Amazon S3.

INCORRECT: “Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the second Region using that EBS volume” is incorrect. You cannot create an EBS volume directly from Amazon S3.

Question 2:

A research group needs a fleet of EC2 instances for a specialized task that must deliver high random I/O performance. Each instance in the fleet would have access to a dataset that is replicated across the instances. Because of the resilient application architecture, the specialized task would continue to be processed even if any instance goes down, as the underlying application architecture would ensure the replacement instance has access to the required dataset.

Which of the following options is the MOST cost-optimal and resource-efficient solution to build this fleet of EC2 instances?

Options

- A. Use EBS based EC2 instances
- B. Use EC2 instances with EFS mount points
- C. Use EC2 instances with access to S3 based storage
- D. Use Instance Store based EC2 instances

Answer: D

Explanation

Correct option:

Use Instance Store based EC2 instances

An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently such as

buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance store volumes are included as part of the instance's usage cost.

As Instance Store based volumes provide high random I/O performance at low cost (as the storage is part of the instance's usage cost) and the resilient architecture can adjust for the loss of any instance, therefore you should use Instance Store based EC2 instances for this use-case.

Incorrect options:

Use EBS based EC2 instances – EBS based volumes would need to use Provisioned IOPS (io1) as the storage type and that would incur additional costs. As we are looking for the most cost-optimal solution, this option is ruled out.

Use EC2 instances with EFS mount points – Using EFS implies that extra resources would have to be provisioned. As we are looking for the most resource-efficient solution, this option is also ruled out.

Use EC2 instances with access to S3 based storage – Using EC2 instances with access to S3 based storage does not deliver high random I/O performance, this option is just added as a distractor.

27. ENI vs ENA vs EFA

Question 1:

A legacy tightly-coupled High Performance Computing (HPC) application will be migrated to AWS. Which network adapter type should be used?

Options:

- A. Elastic Network Adapter (ENA)
- B. Elastic IP Address
- C. Elastic Network Interface (ENI)
- D. Elastic Fabric Adapter (EFA)

Answer: D

Explanation

An Elastic Fabric Adapter is an AWS Elastic Network Adapter (ENA) with added capabilities. The EFA lets you apply the scale, flexibility, and elasticity of the AWS Cloud to tightly-coupled HPC apps. It is ideal for tightly coupled app as it uses the Message Passing Interface (MPI).

CORRECT: “Elastic Fabric Adapter (EFA)” is the correct answer.

INCORRECT: “Elastic Network Interface (ENI)” is incorrect. The ENI is a basic type of adapter and is not the best choice for this use case.

INCORRECT: “Elastic Network Adapter (ENA)” is incorrect. The ENA, which provides Enhanced Networking, does provide high bandwidth and low inter-instance latency but it does not support the features for a tightly-coupled app that the EFA does.

INCORRECT: “Elastic IP Address” is incorrect. An Elastic IP address is just a static public IP address, it is not a type of network adapter.

28. Encrypted Root Device Volumes & Snapshots

29. Spot Instances & Spot Fleets

Question 1:

Your company uses EC2 instances to develop video distribution services. The EC2 instance polls the queue, receives transcoding requests, and uses Amazon Elastic Transcoder to run the transcoding process. If a process is interrupted by one EC2 instance, transcoding is restarted by another instance according to the queue. A lot of video processing backlogs occur during transcoding processing. When they occur, you should help get through these backlogs by increasing the EC2 instance and improving the processing capacity. These instances will only be needed until the backlog is reduced.

Choose the cost-optimal instance type for backlog processing that meets this requirement.

Options:

- A. Reserved instance



- B. On-demand instance
- C. Spot instance
- D. Dedicated instance

Answer: C

Explanation

In Amazon Elastic Transcode, video transcoding jobs start in the order that the pipeline receives the requests. During the job process, many variables such as input file size, resolution, and bit rate affect the conversion speed. For example, a 10-minute video transcoding operation with an iPhone 4 preset is about 5 minutes. When Amazon Elastic Transcode accepts a large number of jobs, the jobs are queued up as a backlog (in the queue).

In this scenario, it is necessary to temporarily increase the number of instances for transcoding processing in order to suppress the occurrence of backlog. The best instance type is Spot Instances because this additional processing need is only temporary. Spot instances are typically used for temporary processing such as batch processing jobs. Therefore, option 3 is the correct answer for this situation.

Option 1 is incorrect. Reserved Instances are an option to purchase EC2 Instances that is discounted because its booked for a long-term use period of 1 or 3 years. It is not suitable for temporary processing like this in the scenario.

Option 2 is incorrect. On-demand instances are also an option, but they do not meet the cost-optimal requirement.

Option 4 is incorrect. Dedicated instances are used when you want to occupy a physical host server. It does not meet the cost optimization requirement due to its high cost.

Question 2:

A company runs a large batch processing job at the end of every quarter. The processing job runs for 5 days and uses 15 Amazon EC2 instances. The processing must run uninterrupted for 5 hours per day. The company is investigating ways to reduce the cost of the batch processing job.

Which pricing model should the company choose?

Options:

- A. Scheduled reserved instances
- B. Reserved instances
- C. Spot block instances
- D. On-demand instances

Answer: C

Explanation

Spot Instances with a defined duration (also known as Spot blocks) are designed not to be interrupted and will run continuously for the duration you select. This makes them ideal for jobs that take a finite time to complete, such as batch processing, encoding and rendering, modeling and analysis, and continuous integration.

Spot Block is the best solution for this job as it only runs once a quarter for 5 days and therefore reserved instances would not be beneficial. Note that the maximum duration of a Spot Block is 6 hours.

CORRECT: “Spot Block Instances” is the correct answer.

INCORRECT: “Reserved Instances” is incorrect. Reserved instances are good for continuously running workloads that run for a period of 1 or 3 years.

INCORRECT: “On-Demand Instances” is incorrect. There is no cost benefit to using on-demand instances.

INCORRECT: “Scheduled Reserved Instances” is incorrect. These reserved instances are ideal for workloads that run for a certain number of hours each day, but not for just 5 days per quarter.

Question 3:

Amazon EC2 instances in a development environment run between 9am and 5pm Monday-Friday. Production instances run 24/7.

Which pricing models should be used? (choose 2)

Options:

- A. Use On-Demand instances for the production environment
- B. Use scheduled reserved instances for the development environment
- C. Use Spot instances for the development environment
- D. Use Reserved instances for the production environment
- E. Use Reserved instances for the development environment

Answer: B & D

Explanation

Scheduled Instances are a good choice for workloads that do not run continuously but do run on a regular schedule. This is ideal for the development environment.

Reserved instances are a good choice for workloads that run continuously. This is a good option for the production environment.

CORRECT: “Use scheduled reserved instances for the development environment” is a correct answer.

CORRECT: “Use Reserved instances for the production environment” is also a correct answer.

INCORRECT: “Use Spot instances for the development environment” is incorrect. Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. Spot instances are not suitable for the development environment as important work may be interrupted.

INCORRECT: “Use Reserved instances for the development environment” is incorrect as they should be used for the production environment.

INCORRECT: “Use On-Demand instances for the production environment” is incorrect. There is no long-term commitment required when you purchase On-Demand Instances. However, you do not get any discount and therefore this is the most expensive option.

Question 4:

A solutions architect is creating a system that will run analytics on financial data for 4 hours a night, 5 days a week. The analysis is expected to run for the same duration and cannot be interrupted once it is started. The system will be required for a minimum of 1 year.

Which type of Amazon EC2 instances should be used to reduce the cost of the system?

Options:

- A. Spot instances
- B. Standard reserved instances
- C. On-demand instances
- D. Scheduled reserved instances

Answer: D

Explanation

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.

CORRECT: “Scheduled Reserved Instances” is the correct answer.

INCORRECT: “Standard Reserved Instances” is incorrect as the workload only runs for 4 hours a day this would be more expensive.

INCORRECT: “On-Demand Instances” is incorrect as this would be much more expensive as there is no discount applied.

INCORRECT: “Spot Instances” is incorrect as the workload cannot be interrupted once started. With Spot instances workloads can be terminated if the Spot price changes or capacity is required.

30. EC2 Hibernate

Question 01:

You have an in-memory database launched on an EC2 instance and you would like to be able to stop and start the EC2 instance without losing the in-memory state of your database. What do you recommend?

- A• Create an AMI from the instance
- B• Mount an in-memory EBS Volume
- C• Use EC2 Instance Hibernate
- D• Use an EC2 Instance Store

Answer: C

Explanation

Correct option:

Use EC2 Instance Hibernate



When you hibernate an instance, AWS signals the operating system to perform hibernation (suspend-to-disk). Hibernation saves the contents from the instance memory (RAM) to your Amazon EBS root volume. AWS then persists the instance's Amazon EBS root volume and any attached Amazon EBS data volumes. When you start your instance: The Amazon EBS root volume is restored to its previous state. The RAM contents are reloaded. The processes that were previously running on the instance are resumed. Previously attached data volumes are reattached and the instance retains its instance ID.

For the given use-case, we must use EC2 Instance Hibernate, which preserves the in-memory state of our EC2 instance upon hibernating it.

Incorrect options:

Create an AMI from the instance – An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances when you need instances with different configurations.

Creating an AMI won't help, because it is a snapshot of an EBS volume, which represents all the files written on disk, not the state of the memory.

Use an EC2 Instance Store – An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.

Using an EC2 Instance Store won't help either, and we can't stop an instance that has an instance store anyway.

Mount an in-memory EBS Volume – Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale.

In-memory EBS volumes don't exist. This option has been added as a distractor.

Question 39:

A Machine Learning research group uses a proprietary computer vision application hosted on an EC2 instance. Every time the instance needs to be stopped and started again, the application takes about 3 minutes to start as some auxiliary software programs need to be executed so that the application can function. The research group would like to minimize the application bootstrap time whenever the system needs to be stopped and then started at a later point in time.

As a solutions architect, which of the following solutions would you recommend for this use-case?

- A• Use EC2 User-Data
- B• Use EC2 Instance Hibernate
- C• Use EC2 Meta-Data
- D• Create an AMI and launch your EC2 instances from that

Answer: B

Explanation

Correct option:

Use EC2 Instance Hibernate

When you hibernate an instance, AWS signals the operating system to perform hibernation (suspend-to-disk). Hibernation saves the contents from the instance memory (RAM) to your Amazon EBS root volume. AWS then persists the instance's Amazon EBS root volume and any attached Amazon EBS data volumes.

When you start your instance:

The Amazon EBS root volume is restored to its previous state

The RAM contents are reloaded

The processes that were previously running on the instance are resumed

Previously attached data volumes are reattached and the instance retains its instance ID

By using EC2 hibernate, we have the capability to resume it at any point of time, with the application already launched, thus helping us cut the 3 minutes start time.

Incorrect options:

Use EC2 User-Data – EC2 instance user data is the data that you specified in the form of a configuration script while launching your instance. Here, the problem is that the application takes 3 minutes to launch, no matter what. EC2 user data won't help us because it's just here to help us execute a list of commands, not speed them up.

Use EC2 Meta-Data – EC2 instance metadata is data about your instance that you can use to configure or manage the running instance. Instance metadata is divided into categories, for example, host name, events, and security groups. The EC2 meta-data is a distractor and can only help us determine some metadata attributes on our EC2 instances.

Create an AMI and launch your EC2 instances from that - An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances when you need instances with different configurations.

Creating an AMI may help with all the system dependencies, but it won't help us with speeding up the application start time.

- 31. Cloud Watch
 - 32. AWS Command Line
 - 33. IAM Roles with EC2
 - 34. Boot Strap Scripts
 - 35. EC2 Instance Meta Data
-

36. EFS

Question 1:

One company is building file storage using AWS. This storage requirement requires the use of data transfer over the NFSv4 protocol.

Choose a storage type that meets this requirement.

Options:

- A. Amazon FSx
- B. EBS
- C. EFS
- D. S3 Standard

Answer: C

Explanation

Amazon EFS uses a file permission model based on the NFSv4 protocol, file locking performance, with a hierarchical directory structure to enable secure access from thousands of EC2 instances and on-premises servers. Therefore, option 3 is the correct answer.

Option 1 is incorrect. Amazon FSx is an NTFS file system that is accessible to up to thousands of compute instances based on the SMB protocol.

Option 2 is incorrect. Amazon Elastic Block Store (EBS) does not use the NFSv4 protocol.

Option 4 is incorrect. S3 can transfer files directly using Secure File Transfer Protocol (SFTP).

Question 2:

Your company operates a set of EC2 instances hosted on AWS. These are all Linux-based instances and require access to shared data via a standard file interface. Since it is used by multiple instances, the storage where the data is stored requires strong integrity and file locking. So, as a Solutions Architect, you are looking for the best storage option.

Choose the best storage option that meets this requirement.

Options:

- A. EFS
- B. S3
- C. EBS
- D. Glacier

Answer: A

Explanation

Option 1 is the correct answer. EFS allows multiple EC2 instances to access the EFS file system and share data at the same time. EFS provides a file system interface and file system access semantics (such as strong consistency and file locks) that allow simultaneous access from up to thousands of Amazon EC2 instances.

Option 2 is incorrect. S3 is an object storage service. S3 can use stored data from anywhere via the Internet API. It can be used from multiple instances, but it cannot meet all requirements, such as file locks.

Option 3 is incorrect. Amazon EBS is a block-level storage service dedicated to Amazon EC2. With the exception of some instances, data cannot be shared between EC2 instances and so does not meet the requirements.

Option 4 is incorrect. Glacier is a storage for medium- to long-term storage and cannot be used for frequently accessed data.

Question 3:

A company is deploying a fleet of Amazon EC2 instances running Linux across multiple Availability Zones within an AWS Region. The application requires a data storage solution that can be accessed by all of the EC2 instances simultaneously. The solution must be highly scalable and easy to implement. The storage must be mounted using the NFS protocol.

Which solution meets these requirements?

Options:

- A. Create an Amazon RDS database and store the data in a BLOB format. Point the application instances to the RDS endpoint
- B. Create an Amazon EFS file system with mount targets in each Availability Zone. Configure the application instances to mount the file system
- C. Create an Amazon EBS volume and use EBS Multi-Attach to mount the volume to all EC2 instances across each Availability Zone
- D. Create an Amazon S3 bucket and create an S3 gateway endpoint to allow access to the file system using the NFS protocol

Answer: B

Explanation

Amazon EFS provides scalable file storage for use with Amazon EC2. You can use an EFS file system as a common data source for workloads and applications running on multiple instances. The EC2 instances can run in multiple AZs within a Region and the NFS protocol is used to mount the file system.

With EFS you can create mount targets in each AZ for lower latency. The application instances in each AZ will mount the file system using the local mount target.

CORRECT: “Create an Amazon EFS file system with mount targets in each Availability Zone. Configure the application instances to mount the file system” is the correct answer.

INCORRECT: “Create an Amazon S3 bucket and create an S3 gateway endpoint to allow access to the file system using the NFS protocol” is incorrect. You cannot use NFS with S3 or with gateway endpoints.

INCORRECT: “Create an Amazon EBS volume and use EBS Multi-Attach to mount the volume to all EC2 instances across each Availability Zone” is incorrect. You cannot use Amazon EBS Multi-Attach across multiple AZs.

INCORRECT: “Create an Amazon RDS database and store the data in a BLOB format. Point the application instances to the RDS endpoint” is incorrect. This is not a suitable storage solution for a file system that is mounted over NFS.

Question 4:

An application is being created that will use Amazon EC2 instances to generate and store data. Another set of EC2 instances will then analyze and modify the data. Storage requirements will be significant and will continue to grow over time. The application architects require a storage solution.

Which actions would meet these needs?

Options:

- A. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances
- B. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances
- C. Store the data in an Amazon EFS filesystem. Mount the file system on the application instances
- D. Store the data in AWS Storage Gateway. Setup AWS Direct Connect between the Gateway appliance and the EC2 instances

Answer: C

Explanation

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

Amazon EFS supports the Network File System version 4 (NFSv4.1 and NFSv4.0) protocol. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, providing a common data source for workloads and applications running on more than one instance or server.

For this scenario, EFS is a great choice as it will provide a scalable file system that can be mounted by multiple EC2 instances and accessed simultaneously.

CORRECT: “Store the data in an Amazon EFS filesystem. Mount the file system on the application instances” is the correct

answer.

INCORRECT: “Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances” is incorrect. Though there is a new feature that allows (EBS multi-attach) that allows attaching multiple Nitro instances to a volume, this is not on the exam yet, and has some specific constraints.

INCORRECT: “Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances” is incorrect as S3 Glacier is not a suitable storage location for live access to data, it is used for archival.

INCORRECT: “Store the data in AWS Storage Gateway. Setup AWS Direct Connect between the Gateway appliance and the EC2 instances” is incorrect. There is no reason to store the data on-premises in a Storage Gateway, using EFS is a much better solution.

Question 19: Skipped

You would like to mount a network file system on Linux instances, where files will be stored and accessed frequently at first, and then infrequently. What solution is the MOST cost-effective?

- S3 Intelligent Tiering
- Glacier Deep Archive
- EFS IA (Correct)
- FSx for Lustre

Explanation

Correct option:

EFS IA

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability.

Amazon EFS Infrequent Access (EFS IA) is a storage class that provides price/performance that is cost-optimized for files, not accessed every day, with storage prices up to 92% lower compared to Amazon EFS Standard. Therefore, this is the correct option.

Incorrect options:

S3 Intelligent Tiering – Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access.

You can't mount a network file system on S3 Intelligent Tiering as it's an object storage service, so this option is incorrect.

Glacier Deep Archive – Amazon S3 Glacier and S3 Glacier Deep Archive are a secure, durable, and extremely low-cost Amazon S3 cloud storage classes for data archiving and long-term backup. They are designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.

You can't mount a network file system on S3 Intelligent Tiering as it's an object storage/archival service, so this option is incorrect.

FSx for Lustre – Amazon FSx for Lustre makes it easy and cost-effective to launch and run the world's most popular high-performance file system. It is used for workloads such as machine learning, high-performance computing (HPC), video processing, and financial modeling. Amazon FSx enables you to use Lustre file systems for any workload where storage speed matters.

FSx for Lustre is a file system better suited for distributed computing for HPC (high-performance computing) and is very expensive

Question 23:

A startup has just developed a video backup service hosted on a fleet of EC2 instances. The EC2 instances are behind an Application Load Balancer and the instances are using EBS volumes for storage. The service provides authenticated users the ability to upload videos that are then saved on the EBS volume attached to a given instance. On the first day of the beta launch, users start complaining that they can see only some of the videos in their uploaded videos backup. Every time the users log into the website, they claim to see a different subset of their uploaded videos.

Which of the following is the MOST optimal solution to make sure that users can view all the uploaded videos? (Select two)

- A• Mount EFS on all EC2 instances. Write a one time job to copy the videos from all EBS volumes to EFS. Modify the application to use EFS for storing the videos
- B• Write a one time job to copy the videos from all EBS volumes to S3 Glacier Deep Archive and then modify the application to use S3 Glacier Deep Archive for storing the videos

- C• Write a one time job to copy the videos from all EBS volumes to S3 and then modify the application to use Amazon S3 standard for storing the videos
- D• Write a one time job to copy the videos from all EBS volumes to DynamoDB and then modify the application to use DynamoDB for storing the videos
- E• Write a one time job to copy the videos from all EBS volumes to RDS and then modify the application to use RDS for storing the videos

Answer: A & C

Explanation

Correct options:

Write a one time job to copy the videos from all EBS volumes to S3 and then modify the application to use Amazon S3 standard for storing the videos

Mount EFS on all EC2 instances. Write a one time job to copy the videos from all EBS volumes to EFS. Modify the application to use EFS for storing the videos

Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale.

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

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

As EBS volumes are attached locally to the EC2 instances, therefore the uploaded videos are tied to specific EC2 instances. Every time the user logs in, they are directed to a different instance and therefore their videos get dispersed across multiple EBS volumes. The correct solution is to use either S3 or EFS to store the user videos.

Incorrect options:

Write a one time job to copy the videos from all EBS volumes to S3 Glacier Deep Archive and then modify the application to use S3 Glacier Deep Archive for storing the videos – Glacier Deep Archive is meant to be used for long term data archival. It cannot be used to serve static content such as videos or images via a web application. So this option is incorrect.

Write a one time job to copy the videos from all EBS volumes to RDS and then modify the application to use RDS for storing the videos – RDS is a relational database and not the right candidate for storing videos.

Write a one time job to copy the videos from all EBS volumes to DynamoDB and then modify the application to use DynamoDB for storing the videos – DynamoDB is a NoSQL database and not the right candidate for storing videos.

37. FSX for Windows & FSX for Lustre

Question 1:

You are considering storage that allows you to share data between multiple EC2 instances. This storage requires the Windows File Server mechanism.

Choose a storage service that can meet this requirement.

Options:

- A. Amazon FSx for windows
- B. EFS
- C. Amazon S3
- D. EBS

Explanation

Option 1 is the correct answer. The service that can use the mechanism of Windows File Server is Amazon FSx for Windows. This is an AWS service that provides a fully managed native Microsoft Windows file system. Building on Windows Server, Amazon FSx provides compatibility and functionality that Microsoft applications depend on. Amazon FSx uses the SMB protocol to provide an NTFS file system accessible to up to thousands of compute instances.

Option 2 is incorrect. EFS is a NAS-type file storage dedicated to AWS. EFS provides a file system interface and file access semantics (such as strong integrity and file locking) that allow simultaneous access from up to thousands of EC2 instances.

instances. It is not compatible with Windows File Server.

Option 3 is incorrect. Amazon S3 is an object storage, not a file storage.

Option 4 is incorrect. EBS is a block storage, not a file storage.

Question 2:

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

Which service should the solutions architect use?

Options:

- A. AWS Storage Gateway
- B. Amazon FSx
- C. Amazon S3
- D. Amazon EFS

Answer: B

Explanation

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.

Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs).

Additionally, Amazon FSx for Windows File Server supports Distributed File System Replication (DFSR) in both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.

CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems.

INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.

INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.

Question 3:

A Microsoft Windows file server farm uses Distributed File System Replication (DFSR) to synchronize data in an on-premises environment. The infrastructure is being migrated to the AWS Cloud.

Which service should the solutions architect use to replace the file server farm?

Options:

- A. Amazon EBS
- B. Amazon FSx
- C. AWS Storage Gateway
- D. Amazon EFS

Answer: B

Explanation

Amazon FSx for Windows file server supports DFS namespaces and DFS replication. This is the best solution for replacing the on-premises infrastructure.

CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect. You cannot replace a Windows file server farm with EFS as it uses a completely different protocol.

INCORRECT: "Amazon EBS" is incorrect. Amazon EBS provides block-based volumes that are attached to EC2 instances. It cannot be used for replacing a shared Windows file server farm using DFSR.

INCORRECT: "AWS Storage Gateway" is incorrect. This service is used for providing cloud storage solutions for on-premises servers. In this case the infrastructure is being migrated into the AWS Cloud.

Question 4:

An Electronic Design Automation (EDA) application produces massive volumes of data that can be divided into t ↑ categories.

The 'hot data' needs to be both processed and stored quickly in a parallel and distributed fashion. The 'cold data' needs to be

kept for reference with quick access for reads and updates at a low cost.

Which of the following AWS services is BEST suited to accelerate the aforementioned chip design process?

Options:

- A. AWS Glue
- B. Amazon EMR
- C. Amazon FSx for Windows File Server
- D. Amazon FSx for Lustre

Answer: D

Explanation

Correct option:

Amazon FSx for Lustre

Amazon FSx for Lustre makes it easy and cost-effective to launch and run the world's most popular high-performance file system. It is used for workloads such as machine learning, high-performance computing (HPC), video processing, and financial modeling. The open-source Lustre file system is designed for applications that require fast storage – where you want your storage to keep up with your compute. FSx for Lustre integrates with Amazon S3, making it easy to process data sets with the Lustre file system. When linked to an S3 bucket, an FSx for Lustre file system transparently presents S3 objects as files and allows you to write changed data back to S3.

FSx for Lustre provides the ability to both process the ‘hot data’ in a parallel and distributed fashion as well as easily store the ‘cold data’ on Amazon S3. Therefore this option is the BEST fit for the given problem statement.

Incorrect options:

Amazon FSx for Windows File Server – Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Service Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. FSx for Windows does not allow you to present S3 objects as files and does not allow you to write changed data back to S3. Therefore you cannot reference the “cold data” with quick access for reads and updates at low cost. Hence this option is not correct.

Amazon EMR – Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. Amazon EMR uses Hadoop, an open-source framework, to distribute your data and processing across a resizable cluster of Amazon EC2 instances. EMR does not offer the same storage and processing speed as FSx for Lustre. So it is not the right fit for the given high-performance workflow scenario.

AWS Glue – 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 Glue job is meant to be used for batch ETL data processing. AWS Glue does not offer the same storage and processing speed as FSx for Lustre. So it is not the right fit for the given high-performance workflow scenario.

Question 5:

A large financial institution operates an on-premises data center with hundreds of PB of data managed on Microsoft’s Distributed File System (DFS). The CTO wants the organization to transition into a hybrid cloud environment and run data-intensive analytics workloads that support DFS.

Which of the following AWS services can facilitate the migration of these workloads?

Options:

- A. AWS Managed Microsoft AD
- B. Amazon FSx for Windows File Server
- C. Amazon FSx for Lustre
- D. Microsoft SQL Server on Amazon

Answer: B

Explanation

Correct option:

Amazon FSx for Windows File Server

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Service Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. Amazon FSx supports the use of Microsoft’s Distributed File System (DFS) to organize shares into a single folder structure up to hundreds of PB in size. So this option is correct.

Incorrect options:**Amazon FSx for Lustre**

Amazon FSx for Lustre makes it easy and cost-effective to launch and run the world's most popular high-performance file system. It is used for workloads such as machine learning, high-performance computing (HPC), video processing, and financial modeling. Amazon FSx enables you to use Lustre file systems for any workload where storage speed matters. FSx for Lustre does not support Microsoft's Distributed File System (DFS), so this option is incorrect.

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. AWS Managed Microsoft AD is built on the actual Microsoft Active Directory and does not require you to synchronize or replicate data from your existing Active Directory to the cloud. AWS Managed Microsoft AD does not support Microsoft's Distributed File System (DFS), so this option is incorrect.

Microsoft SQL Server on Amazon

Microsoft SQL Server on AWS offers you the flexibility to run Microsoft SQL Server database on AWS Cloud. Microsoft SQL Server on AWS does not support Microsoft's Distributed File System (DFS), so this option is incorrect.

Question 15: Skipped

Your company has an on-premises Distributed File System Replication (DFSR) service to keep files synchronized on multiple Windows servers, and would like to migrate to AWS cloud.

What do you recommend as a replacement for the DFSR?

- Amazon S3
- EFS
- FSx for Windows (Correct)
- FSx for Lustre

Explanation**Correct option:****FSx for Windows**

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Service Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. The Distributed File System Replication (DFSR) service is a new multi-master replication engine that is used to keep folders synchronized on multiple servers. Amazon FSx supports the use of Microsoft's Distributed File System (DFS) to organize shares into a single folder structure up to hundreds of PB in size.

FSx for Windows is a perfect distributed file system, with replication capability, and can be mounted on Windows.

Incorrect options:

FSx for Lustre - Amazon FSx for Lustre makes it easy and cost-effective to launch and run the world's most popular high-performance file system. It is used for workloads such as machine learning, high-performance computing (HPC), video processing, and financial modeling. The open-source Lustre file system is designed for applications that require fast storage – where you want your storage to keep up with your compute. Amazon FSx enables you to use Lustre file systems for any workload where storage speed matters. FSx for Lustre integrates with Amazon S3, making it easy to process data sets with the Lustre file system.

FSx for Lustre is for Linux only, so this option is incorrect.

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

EFS is a network file system but for Linux only, so this option is incorrect.

Amazon S3 - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Amazon S3 cannot be mounted as a file system on Windows, so this option is incorrect.



39. HPC

Question 01:

An ivy-league university is assisting NASA to find potential landing sites for exploration vehicles of unmanned missions to our neighboring planets. The university uses High Performance Computing (HPC) driven application architecture to identify these landing sites.

Which of the following EC2 instance topologies should this application be deployed on?

Options:

- A. The EC2 instances should be deployed in a partition placement group so that distributed workloads can be handled effectively
- B. The EC2 instances should be deployed in a cluster placement group so that the underlying workload can benefit from low network latency and high network throughput
- C. The EC2 instances should be deployed in a spread placement group so that there are no correlated failures
- D. The EC2 instances should be deployed in an Auto Scaling group so that application meets high availability requirements

Answer: B

Explanation

Correct option:

The EC2 instances should be deployed in a cluster placement group so that the underlying workload can benefit from low network latency and high network throughput

The key thing to understand in this question is that HPC workloads need to achieve low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications. Cluster placement groups pack instances close together inside an Availability Zone. These are recommended for applications that benefit from low network latency, high network throughput, or both. Therefore this option is the correct answer.

Incorrect options:

The EC2 instances should be deployed in a partition placement group so that distributed workloads can be handled effectively – A partition placement group spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka. A partition placement group can have a maximum of seven partitions per Availability Zone. Since a partition placement group can have partitions in multiple Availability Zones in the same region, therefore instances will not have low-latency network performance. Hence the partition placement group is not the right fit for HPC applications.

The EC2 instances should be deployed in a spread placement group so that there are no correlated failures – A spread placement group is a group of instances that are each placed on distinct racks, with each rack having its own network and power source. The instances are placed across distinct underlying hardware to reduce correlated failures. You can have a maximum of seven running instances per Availability Zone per group. Since a spread placement group can span multiple Availability Zones in the same Region, therefore instances will not have low-latency network performance. Hence spread placement group is not the right fit for HPC applications.

The EC2 instances should be deployed in an Auto Scaling group so that application meets high availability requirements – An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling. You do not use Auto Scaling groups per se to meet HPC requirements.

40. WAF

Question 1:

Your company uses S3 as storage for data and runs an application that provides S3 objects to users. As an application administrator, you recently discovered that the URL links for the data provided by this application are being used without permission. You need to address this issue by making external links permanently unavailable.

Select the service you need for this requirement.

Options:

- A. Deliver data as an object with a pre-signed URL
- B. Apply Referrer restrictions for links provided by AWS WAF
- C. Deliver data as an object with signed cookies
- D. Restrict delivery by encrypting access processing to S3



Answer: B

Explanation

You can configure content delivery with CloudFront on S3 and leverage AWS WAF to implement Referrer limits. AWS WAF is a web application firewall that monitors HTTP and HTTPS requests forwarded to CloudFront and allows you to control access to your content. You can restrict the direct reference of URL links by the Referrer restriction of AWS WAF. Therefore, option 2 is the correct answer.

Options 1 and 3 are incorrect. CloudFront signed URLs and signed cookies provide much the same functionality and give you control over who can access your content. However, it is not correct because you cannot permanently prohibit direct links.

Option 4 is incorrect. It is not possible to restrict distribution by encrypting the access process to S3.

Question 2:

A media company runs a photo-sharing web application that is accessed across three different countries. The application is deployed on several Amazon EC2 instances running behind an Application Load Balancer. With new government regulations, the company has been asked to block access from two countries and allow access only from the home country of the company.

Which configuration should be used to meet this changed requirement?

Options:

- A. Use Geo Restriction feature of Amazon CloudFront in a VPC
- B. Configure the security group for the EC2 instances
- C. Configure the security group on the Application Load Balancer
- D. Configure AWS WAF on the Application Load Balancer in a VPC

Answer: D

Explanation

Correct option:

AWS WAF is a web application firewall service that lets you monitor web requests and protect your web applications from malicious requests. Use AWS WAF to block or allow requests based on conditions that you specify, such as the IP addresses. You can also use AWS WAF preconfigured protections to block common attacks like SQL injection or cross-site scripting.

Configure AWS WAF on the Application Load Balancer in a VPC

You can use AWS WAF with your Application Load Balancer to allow or block requests based on the rules in a web access control list (web ACL). Geographic (Geo) Match Conditions in AWS WAF allows you to use AWS WAF to restrict application access based on the geographic location of your viewers. With geo match conditions you can choose the countries from which AWS WAF should allow access.

Geo match conditions are important for many customers. For example, legal and licensing requirements restrict some customers from delivering their applications outside certain countries. These customers can configure a whitelist that allows only viewers in those countries. Other customers need to prevent the downloading of their encrypted software by users in certain countries. These customers can configure a blacklist so that end-users from those countries are blocked from downloading their software.

Incorrect options:

Use Geo Restriction feature of Amazon CloudFront in a VPC – Geo Restriction feature of CloudFront helps in restricting traffic based on the user's geographic location. But, CloudFront works from edge locations and doesn't belong to a VPC. Hence, this option itself is incorrect and given only as a distractor.

Configure the security group on the Application Load Balancer

Configure the security group for the EC2 instances

Security Groups cannot restrict access based on the user's geographic location.

Question 24:

To improve the performance and security of the application, the engineering team at a company has created a CloudFront distribution with an Application Load Balancer as the custom origin. The team has also set up a Web Application Firewall (WAF) with CloudFront distribution. The security team at the company has noticed a surge in malicious attacks from a specific IP address to steal sensitive data stored on the EC2 instances.

As a solutions architect, which of the following actions would you recommend to stop the attacks?

- A• Create a ticket with AWS support to take action against the malicious IP
- B• Create a deny rule for the malicious IP in the NACL associated with each of the instances
- C• Create a deny rule for the malicious IP in the Security Groups associated with each of the instances
- D• Create an IP match condition in the WAF to block the malicious IP address

Answer: D

Explanation

Correct option:

Create an IP match condition in the WAF to block the malicious IP address

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define.

If you want to allow or block web requests based on the IP addresses that the requests originate from, create one or more IP match conditions. An IP match condition lists up to 10,000 IP addresses or IP address ranges that your requests originate from. So, this option is correct.

Incorrect options:

Create a deny rule for the malicious IP in the NACL associated with each of the instances – NACLs are not associated with instances. So this option is also ruled out.

Create a deny rule for the malicious IP in the Security Groups associated with each of the instances – You cannot deny rules in Security Groups. So this option is ruled out.

Create a ticket with AWS support to take action against the malicious IP – Managing the security of your application is your responsibility, not that of AWS, so you cannot raise a ticket for this issue.

41. Databases

42. Create an RDS Instance

Question 1:

Your company uses an Amazon RDS MySQL database. As a Solutions Architect, you have changed your settings to create a read-only read replica and it seems to handle the heavy read load of the database. However, there is an event where old data is being displayed in the report at a certain time.

What are the most likely root causes of this problem?

Options:

- A. Since it is a multi-AZ configuration of RDS, the RDS data in another AZ is still old
- B. Old data may be displayed due to replication lag
- C. The read replica is not set up properly
- D. The backup of the original DB has not been set up properly

Answer: B

Explanation

Because Read Replicas are separate database instances that are asynchronously replicated, you may not be able to see some of the latest transactions due to delays in replication data. This is called the replication lag. Therefore, option 2 is the correct answer.

Option 1 is incorrect. The RDS multi-AZ configuration does not utilize the secondary database unless a failover is performed, so the multi-AZ configuration does not affect data processing.

Option 3 is incorrect. Data becoming old due to the misconfiguration of the read replica does not occur.

Option 4 is incorrect. Even if the backup of the master DB instance is not successfully obtained, it does not affect normal data processing.

Question 2:

As a Solutions Architect, you plan to use your RDS instance as a database for your applications. To meet your security requirements, you need to ensure that the data stored in your database is encrypted.

What should I do to achieve this requirement?

Options:

- A. Enable server-side encryption when configuring RDS
- B. Choose a volume that is automatically encrypted when you are to select an EBS volume
- C. Enable encryption by choosing an appropriate cluster configuration

D. Enable encryption by setting the security group**Answer: A****Explanation**

Database encryption can be done during the database creation. To encrypt your Amazon RDS DB instance and snapshot, enable the encryption option in the Amazon RDS DB Instance Settings menu. Data to be encrypted includes DB instances, automatic backups, read replicas, and snapshots. Therefore, option 1 is the correct answer.

Option 2 is incorrect. EBS volumes are independent of RDS and are not used to encrypt RDS data.

Option 3 is incorrect. Cluster configuration have nothing to do with encryption. The cluster configuration are a setting for making read processing highly available.

Option 4 is incorrect. Security groups are used for traffic control and are not related to encryption.

Question 3:

A company uses an Amazon RDS MySQL database instance to store customer order data. The security team have requested that SSL/TLS encryption in transit must be used for encrypting connections to the database from application servers. The data in the database is currently encrypted at rest using an AWS KMS key.

How can a Solutions Architect enable encryption in transit?

Options:

- A. Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption in transit enabled
- B. Download the AWS-provided root certificates. Use the certificates when connecting to the RDS DB instance
- C. Add a self-signed certificate to the RDS DB instance. Use the certificates in all connections to the RDS DB instance
- D. Enable encryption in transit using the RDS Management console and obtain a key using AWS KMS

Answer: B**Explanation**

Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

You can download a root certificate from AWS that works for all Regions or you can download Region-specific intermediate certificates.

CORRECT: “Download the AWS-provided root certificates. Use the certificates when connecting to the RDS DB instance” is the correct answer.

INCORRECT: “Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption in transit enabled” is incorrect. There is no need to do this as a certificate is created when the DB instances is launched.

INCORRECT: “Enable encryption in transit using the RDS Management console and obtain a key using AWS KMS” is incorrect. You cannot enable/disable encryption in transit using the RDS management console or use a KMS key.

INCORRECT: “Add a self-signed certificate to the RDS DB instance. Use the certificates in all connections to the RDS DB instance” is incorrect. You cannot use self-signed certificates with RDS.

Question 4:

A company runs an application that uses an Amazon RDS PostgreSQL database. The database is currently not encrypted. A Solutions Architect has been instructed that due to new compliance requirements all existing and new data in the database must be encrypted. The database experiences high volumes of changes and no data can be lost.

How can the Solutions Architect enable encryption for the database without incurring any data loss?

Options:

- A. Create an RDS read replica and specify an encryption key. Promote the encrypted read replica to primary. Update the application to point to the new RDS DB endpoint
- B. Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs
- C. Update the RDS DB to Multi-AZ mode and enable encryption for the standby replica. Perform a failover to the standby instance and then delete the unencrypted RDS DB instance
- D. Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot. Configure the application to use the new DB endpoint

Answer: B**Explanation**

You cannot change the encryption status of an existing RDS DB instance. Encryption must be specified when creating the RDS DB instance. The best way to encrypt an existing database is to take a snapshot, encrypt a copy of the snapshot and restore the snapshot to a new RDS DB instance. This results in an encrypted database that is a new instance. Applications must be updated to use the new RDS DB endpoint.

In this scenario as there is a high rate of change, the databases will be out of sync by the time the new copy is created and is functional. The best way to capture the changes between the source (unencrypted) and destination (encrypted) DB is to use AWS Database Migration Service (DMS) to synchronize the data.

CORRECT: “Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs” is the correct answer.

INCORRECT: “Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot. Configure the application to use the new DB endpoint” is incorrect. This answer creates an encrypted DB instance but does not synchronize the data.

INCORRECT: “Create an RDS read replica and specify an encryption key. Promote the encrypted read replica to primary. Update the application to point to the new RDS DB endpoint” is incorrect. You cannot create an encrypted read replica of an unencrypted RDS DB. The read replica will always have the same encryption status as the RDS DB it is created from.

INCORRECT: “Update the RDS DB to Multi-AZ mode and enable encryption for the standby replica. Perform a failover to the standby instance and then delete the unencrypted RDS DB instance” is incorrect. You also cannot have an encrypted Multi-AZ standby instance of an unencrypted RDS DB.

Question 29:

A retail company wants to share sensitive accounting data that is stored in an Amazon RDS DB instance with an external auditor. The auditor has its own AWS account and needs its own copy of the database.

Which of the following would you recommend to securely share the database with the auditor?

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

Answer: D

Explanation

Correct option:

Create an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key

You can share the AWS Key Management Service (AWS KMS) customer master key (CMK) that was used to encrypt the snapshot with any accounts that you want to be able to access the snapshot. You can share AWS KMS CMKs with another AWS account by adding the other account to the AWS KMS key policy.

Making an encrypted snapshot of the database will give the auditor a copy of the database, as required for the given use case.

Incorrect options:

Create a snapshot of the database in Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket
- RDS stores the DB snapshots in the Amazon S3 bucket belonging to the same AWS region where the RDS instance is located. RDS stores these on your behalf and you do not have direct access to these snapshots in S3, so it's not possible to grant access to the snapshot objects in S3.

Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket - This solution is feasible though not optimal. It requires a lot of unnecessary work and is difficult to audit when such bulk data is exported into text files.

Set up a read replica of the database and configure IAM standard database authentication to grant the auditor access - Read Replicas make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Creating Read Replicas for audit purposes is overkill. Also, the question mentions that the auditor needs to have their own copy of the database, which is not possible with replicas.

Question 33:

An IT company is working on a client project to build a Supply Chain Management application. The web-tier of the application runs on an EC2 instance and the database tier is on Amazon RDS MySQL. For beta testing, all the resources are currently deployed in a single Availability Zone. The development team wants to improve application availability before the go-live.

Given that all end users of the web application would be located in the US, which of the following would be the MOST resource-efficient solution?

- A• Deploy the web-tier EC2 instances in two Availability Zones, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in read replica configuration
- B• Deploy the web-tier EC2 instances in two Availability Zones, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration
- C• Deploy the web-tier EC2 instances in two regions, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in read replica configuration
- D• Deploy the web-tier EC2 instances in two regions, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration

Answer: B

Explanation

Correct option:

Deploy the web-tier EC2 instances in two Availability Zones, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Therefore, deploying the web-tier EC2 instances in two Availability Zones, behind an Elastic Load Balancer would improve the availability of the application.

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Deploying the Amazon RDS MySQL database in Multi-AZ configuration would improve availability and hence this is the correct option.

Incorrect options:

Deploy the web-tier EC2 instances in two Availability Zones, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in read replica configuration

Deploy the web-tier EC2 instances in two regions, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in read replica configuration

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Read replicas are meant to address scalability issues. You cannot use read replicas for improving availability, so both these options are incorrect.

Deploy the web-tier EC2 instances in two regions, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration – As Elastic Load Balancing does not work across regions, so this option is incorrect.

43. RDS Backups, Multi-AZ & Read Replicas

Question 1:

Your company has an application that consists of ELB, EC2 instances, and an RDS database. Recently, the number of read requests to the RDS database has been increasing, resulting in poor performance.

Select the changes you should make to your architecture to improve RDS performance.

Options:

- A. Install CloudFront before accessing the DB
- B. Improve processing by making RDS a multi-AZ configuration
- C. Increase read replicas of RDS
- D. Place DynamoDB as a cache layer in front of the RDS DB

Answer: C

Explanation

Adding a Read Replica to Amazon RDS improves the performance and durability of the database (DB) instance read process. This feature allows you to stretch and scale the capacity of a single DB instance to ease the overall workload of frequently read databases. You can create up to 5 Read Replicas for your RDS DB instance. It can support high volume read traffic for your application and improve overall read throughput. Therefore, option 3 is the correct answer.

Option 1 is incorrect because CloudFront is used to speed up global content delivery processing, not to improve database reading processing.

Option 2 is incorrect. You can improve the availability of your DB instance by configuring RDS in a multi-AZ configuration, but it will not improve read performance.

Option 4 is incorrect. By installing ElastiCache in front of RDS instead of DynamoDB, it is possible to improve read performance by cache processing. However DynamoDB is not a suitable solution.

Question 2:

An Amazon RDS Read Replica is being deployed in a separate region. The master database is not encrypted but all data in the new region must be encrypted. How can this be achieved?

Options:

- A. Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica
- B. Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica
- C. Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot
- D. Enabled encryption on the master DB instance, then create an encrypted cross-region Read Replica

Answer: A

Explanation

You cannot create an encrypted Read Replica from an unencrypted master DB instance. You also cannot enable encryption after launch time for the master DB instance. Therefore, you must create a new master DB by taking a snapshot of the existing DB, encrypting it, and then creating the new DB from the snapshot. You can then create the encrypted cross-region Read Replica of the master DB.

CORRECT: “Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica” is the correct answer.

INCORRECT: “Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica” is incorrect. All other options will not work due to the limitations explained above.

INCORRECT: “Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot” is incorrect. All other options will not work due to the limitations explained above.

INCORRECT: “Enabled encryption on the master DB instance, then create an encrypted cross-region Read Replica” is incorrect. All other options will not work due to the limitations explained above.

Question 3:

A new DevOps engineer has just joined a development team and wants to understand the replication capabilities for RDS Multi-AZ as well as RDS Read-replicas.

Which of the following correctly summarizes these capabilities for the given database?

Options:

- A. Multi-AZ follows asynchronous replication and spans one Availability Zone within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region
- B. Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region
- C. Multi-AZ follows synchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region
- D. Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

Answer: C

Explanation

Correct option:

Multi-AZ follows synchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Multi-AZ spans at least two Availability Zones within a single region.

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance.

Amazon RDS replicates all databases in the source DB instance. Read replicas can be within an Availability Zone, Cross-AZ, or Cross-Region.

Incorrect Options:

Multi-AZ follows asynchronous replication and spans one Availability Zone within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

These three options contradict the earlier details provided in the explanation. To summarize, Multi-AZ follows synchronous replication for RDS. Hence these options are incorrect.

Question 6: Skipped

The engineering manager for a content management application wants to set up RDS read replicas to provide enhanced performance and read scalability. The manager wants to understand the data transfer charges while setting up RDS read replicas.

Which of the following would you identify as correct regarding the data transfer charges for RDS read replicas?

- There are data transfer charges for replicating data across AWS Regions (Correct)
- There are data transfer charges for replicating data within the same AWS Region
- There are no data transfer charges for replicating data across AWS Regions
- There are data transfer charges for replicating data within the same Availability Zone

Explanation

Correct option:

There are data transfer charges for replicating data across AWS Regions

RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

A read replica is billed as a standard DB Instance and at the same rates. You are not charged for the data transfer incurred in replicating data between your source DB instance and read replica within the same AWS Region.

Incorrect options:

There are data transfer charges for replicating data within the same Availability Zone

There are data transfer charges for replicating data within the same AWS Region

There are no data transfer charges for replicating data across AWS Regions

These three options contradict the explanation provided above, so these options are incorrect.

Question 21:

What is true about RDS Read Replicas encryption?

- A• If the master database is encrypted, the read replicas can be either encrypted or unencrypted
- B• If the master database is unencrypted, the read replicas are encrypted
- C• If the master database is unencrypted, the read replicas can be either encrypted or unencrypted
- D• If the master database is encrypted, the read replicas are encrypted

Answer: D

Explanation

Correct option:

If the master database is encrypted, the read replicas are encrypted

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They r ↑ it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. For the MySQL,

MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. read replicas can be within an Availability Zone, Cross-AZ, or Cross-Region.

On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots. Therefore, this option is correct.

Incorrect options:

If the master database is encrypted, the read replicas can be either encrypted or unencrypted - If the master database is encrypted, the read replicas are necessarily encrypted, so this option is incorrect.

If the master database is unencrypted, the read replicas can be either encrypted or unencrypted

If the master database is unencrypted, the read replicas are encrypted

If the master database is not encrypted, the read replicas cannot be encrypted, so both these options are incorrect.

44. Dynamo DB

Question 1:

Your company needs to use a fully managed NoSQL database on the AWS cloud. The database is required to be configured for backup and have high availability.

Which database meets this requirement?

Options:

- A. Amazon Aurora
- B. RDS
- C. Dynamo DB
- D. Redshift

Answer: C

Explanation

Amazon DynamoDB is a fully managed NoSQL database service that provides seamless, scalable, fast and predictable performance. Therefore, option 3 is the correct answer to meet the requirements.

Option 1 is incorrect. Amazon RDS is a managed relational database and is so incorrect.

Option 2 is incorrect. Amazon Aurora is a relational database built for the cloud that is compatible with MySQL and PostgreSQL and is incorrect.

Option 4 is incorrect. Amazon Redshift is a fast, simple and cost-effective data warehouse service that doesn't meet your requirements.

Question 2:

Your company is developing a new mobile application on AWS. Currently, as a Solutions Architect, you are considering how to save your user settings. The size of the individual custom data will be approximately 10KB. It is estimated that tens of thousands of customers will use this mobile application during the release phase. High-speed processing using this user setting data is required. The datastore that stores user settings should be cost-effective, highly available, scalable, and secure.

Choose the best database to meet this requirement.

Options:

- A. Accumulate user settings using RDS
- B. Accumulate user settings using S3
- C. Accumulate user setting using Redshift cluster
- D. Accumulate user settings using DynamoDB

Answer: D

Explanation

In this scenario, the size of the individual custom data will be approximately 10KB. It is best to use a NoSQL database to store and process such small data. On AWS, DynamoDB is an ideal database service for storing session data, user settings, metadata, and more. DynamoDB is a highly scalable managed service that can meet this requirement. It is estimated that tens of thousands of customers will use this mobile application during the release phase. Since high-speed processing using this user setting data may be required, NoSQL type high-speed processing in DynamoDB is optimal. Therefore, option 4 is the correct ansv ↑

Option 1 is incorrect. Although it is possible to store user-configured data in RDS, DynamoDB is the best choice for high-speed

processing of data volumes and mobile applications.

Option 2 is incorrect. S3 is not suitable for high-speed processing of data volumes and mobile applications. S3 is used for data storage such as objects, not data processing.

Option 3 is incorrect. Redshift is a relational database type data warehouse used for data analysis. NoSQL type DynamoDB is more suitable for retaining user settings and fast processing.

Question 3:

An Amazon VPC contains several Amazon EC2 instances. The instances need to make API calls to Amazon DynamoDB. A solutions architect needs to ensure that the API calls do not traverse the internet.

How can this be accomplished? (Select TWO.)

Options:

- A. Create a new DynamoDB table that uses the endpoint
- B. Create a VPC peering connection between the VPC and DynamoDB
- C. Create an ENI for the endpoint in each of the subnets of the VPC
- D. Create a gateway endpoint for DynamoDB
- E. Create a route table entry for the endpoint

Answer: D & E

Explanation

Amazon DynamoDB and Amazon S3 support gateway endpoints, not interface endpoints. With a gateway endpoint you create the endpoint in the VPC, attach a policy allowing access to the service, and then specify the route table to create a route table entry in.

CORRECT: “Create a route table entry for the endpoint” is a correct answer.

CORRECT: “Create a gateway endpoint for DynamoDB” is also a correct answer.

INCORRECT: “Create a new DynamoDB table that uses the endpoint” is incorrect as it is not necessary to create a new DynamoDB table.

INCORRECT: “Create an ENI for the endpoint in each of the subnets of the VPC” is incorrect as an ENI is used by an interface endpoint, not a gateway endpoint.

INCORRECT: “Create a VPC peering connection between the VPC and DynamoDB” is incorrect as you cannot create a VPC peering connection between a VPC and a public AWS service as public services are outside of VPCs.

Question 18: Skipped

A social photo-sharing web application is hosted on EC2 instances behind an Elastic Load Balancer. The app gives the users the ability to upload their photos and also shows a leaderboard on the homepage of the app. The uploaded photos are stored in S3 and the leaderboard data is maintained in DynamoDB. The EC2 instances need to access both S3 and DynamoDB for these features.

As a solutions architect, which of the following solutions would you recommend as the MOST secure option?

- Save the AWS credentials (access key Id and secret access token) in a configuration file within the application code on the EC2 instances. EC2 instances can use these credentials to access S3 and DynamoDB
- Attach the appropriate IAM role to the EC2 instance profile so that the instance can access S3 and DynamoDB (Correct)
- Configure AWS CLI on the EC2 instances using a valid IAM user’s credentials. The application code can then invoke shell scripts to access S3 and DynamoDB via AWS CLI
- Encrypt the AWS credentials via a custom encryption library and save it in a secret directory on the EC2 instances. The application code can then safely decrypt the AWS credentials to make the API calls to S3 and DynamoDB

Explanation

Correct option:

Attach the appropriate IAM role to the EC2 instance profile so that the instance can access S3 and DynamoDB

Applications that run on an EC2 instance must include AWS credentials in their AWS API requests. You could have your developers store AWS credentials directly within the EC2 instance and allow applications in that instance to use those credentials. But developers would then have to manage the credentials and ensure that they securely pass the credentials to each instance and update each EC2 instance when it’s time to rotate the credentials.

Instead, you should use an IAM role to manage temporary credentials for applications that run on an EC2 instance. When you use a role, you don’t have to distribute long-term credentials (such as a username and password or access keys) to an EC2 instance.

The role supplies temporary permissions that applications can use when they make calls to other AWS resources. When you launch an EC2 instance, you specify an IAM role to associate with the instance. Applications that run on the instance can then use the role-supplied temporary credentials to sign API requests. Therefore, this option is correct.

Incorrect options:

Save the AWS credentials (access key Id and secret access token) in a configuration file within the application code on the EC2 instances. EC2 instances can use these credentials to access S3 and DynamoDB

Configure AWS CLI on the EC2 instances using a valid IAM user's credentials. The application code can then invoke shell scripts to access S3 and DynamoDB via AWS CLI

Encrypt the AWS credentials via a custom encryption library and save it in a secret directory on the EC2 instances. The application code can then safely decrypt the AWS credentials to make the API calls to S3 and DynamoDB

Keeping the AWS credentials (encrypted or plain text) on the EC2 instance is a bad security practice, therefore these three options using the AWS credentials are incorrect.

45. Advanced Dynamo DB

Question 1:

A retail company has developed a REST API which is deployed in an Auto Scaling group behind an Application Load Balancer. The API stores the user data in DynamoDB and any static content, such as images, are served via S3. On analyzing the usage trends, it is found that 90% of the read requests are for commonly accessed data across all users.

As a Solutions Architect, which of the following would you suggest as the MOST efficient solution to improve the application performance?

Options:

- A. Enable ElastiCache Redis for DynamoDB and CloudFront for S3
- B. Enable DAX for DynamoDB and ElastiCache Memcached for S3
- C. Enable DynamoDB Accelerator (DAX) for DynamoDB and CloudFront for S3
- D. Enable ElastiCache Redis for DynamoDB and ElastiCache Memcached for S3

Answer: C

Explanation**Correct option:**

Enable DynamoDB Accelerator (DAX) for DynamoDB and CloudFront for S3

DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB that delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second.

DAX is tightly integrated with DynamoDB—you simply provision a DAX cluster, use the DAX client SDK to point your existing DynamoDB API calls at the DAX cluster, and let DAX handle the rest. Because DAX is API-compatible with DynamoDB, you don't have to make any functional application code changes. DAX is used to natively cache DynamoDB reads.

CloudFront is a content delivery network (CDN) service that delivers static and dynamic web content, video streams, and APIs around the world, securely and at scale. By design, delivering data out of CloudFront can be more cost-effective than delivering it from S3 directly to your users.

When a user requests content that you serve with CloudFront, their request is routed to a nearby Edge Location. If CloudFront has a cached copy of the requested file, CloudFront delivers it to the user, providing a fast (low-latency) response. If the file they've requested isn't yet cached, CloudFront retrieves it from your origin – for example, the S3 bucket where you've stored your content.

So, you can use CloudFront to improve application performance to serve static content from S3.

Incorrect options:

Enable ElastiCache Redis for DynamoDB and CloudFront for S3

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. Amazon ElastiCache for Redis is a great choice for real-time transactional and analytical processing use cases such as caching, chat/messaging, gaming leaderboards, geospatial, machine learning, media streaming, queues, real-time analytics, and session store.

Although you can integrate Redis with DynamoDB, it's much more involved than using DAX which is a much better fit.

Enable DAX for DynamoDB and ElastiCache Memcached for S3

Enable ElastiCache Redis for DynamoDB and ElastiCache Memcached for S3

Amazon ElastiCache for Memcached is a Memcached-compatible in-memory key-value store service that can be used as a cache

or a data store. Amazon ElastiCache for Memcached is a great choice for implementing an in-memory cache to decrease access latency, increase throughput, and ease the load off your relational or NoSQL database.

ElastiCache cannot be used as a cache to serve static content from S3, so both these options are incorrect.

Question 2:

The engineering team at an in-home fitness company is evaluating multiple in-memory data stores with the ability to power its on-demand, live leaderboard. The company's leaderboard requires high availability, low latency, and real-time processing to deliver customizable user data for the community of users working out together virtually from the comfort of their home.

As a solutions architect, which of the following solutions would you recommend? (Select two)

Options:

- A. Power the on-demand, live leaderboard using DynamoDB with DynamoDB Accelerator (DAX) as it meets the in-memory, high availability, low latency requirements
- B. Power the on-demand, live leaderboard using AWS Neptune as it meets the in-memory, high availability, low latency requirements
- C. Power the on-demand, live leaderboard using DynamoDB as it meets the in-memory, high availability, low latency requirements
- D. Power the on-demand, live leaderboard using RDS Aurora as it meets the in-memory, high availability, low latency requirements
- E. Power the on-demand, live leaderboard using ElastiCache Redis as it meets the in-memory, high availability, low latency requirements

Answer: E

Explanation

Correct options:

Power the on-demand, live leaderboard using ElastiCache Redis as it meets the in-memory, high availability, low latency requirements

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. Amazon ElastiCache for Redis is a great choice for real-time transactional and analytical processing use cases such as caching, chat/messaging, gaming leaderboards, geospatial, machine learning, media streaming, queues, real-time analytics, and session store. ElastiCache for Redis can be used to power the live leaderboard, so this option is correct.

Power the on-demand, live leaderboard using DynamoDB with DynamoDB Accelerator (DAX) as it meets the in-memory, high availability, low latency requirements

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multiregion, multimaster, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DAX is a DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding applications. So DynamoDB with DAX can be used to power the live leaderboard.

Incorrect options:

Power the on-demand, live leaderboard using AWS Neptune as it meets the in-memory, high availability, low latency requirements - Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets. Neptune is not an in-memory database, so this option is not correct.

Power the on-demand, live leaderboard using DynamoDB as it meets the in-memory, high availability, low latency requirements - DynamoDB is not an in-memory database, so this option is not correct.

Power the on-demand, live leaderboard using RDS Aurora as it meets the in-memory, high availability, low latency requirements - Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. Aurora is not an in-memory database, so this option is not correct.

Question 03:

A company uses DynamoDB as a data store for various kinds of customer data, such as user profiles, user events, clicks, and visited links. Some of these use-cases require a high request rate (millions of requests per second), low predictable latency, and reliability. The company now wants to add a caching layer to support high read volumes.

As a solutions architect, which of the following AWS services would you recommend as a caching layer for this use ? (Select two)

Options:

- A. DynamoDB Accelerator (DAX)
- B. ElastiCache
- C. Elasticsearch
- D. RDS
- E. Redshift

Answer: A & B

Explanation

Correct options:

DynamoDB Accelerator (DAX) – Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second. DAX does all the heavy lifting required to add in-memory acceleration to your DynamoDB tables, without requiring developers to manage cache invalidation, data population, or cluster management. Therefore, this is a correct option.

ElastiCache – Amazon ElastiCache for Memcached is an ideal front-end for data stores like Amazon RDS or Amazon DynamoDB, providing a high-performance middle tier for applications with extremely high request rates and/or low latency requirements. Therefore, this is also a correct option.

Incorrect options:

RDS – Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. RDS cannot be used as a caching layer for DynamoDB.

Elasticsearch – Elasticsearch is a search engine based on the Lucene library. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents. It cannot be used as a caching layer for DynamoDB.

Redshift – Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for large scale data set storage and analysis. It cannot be used as a caching layer for DynamoDB.

46. Redshift

Question 1:

As a solutions architect, you are building a business analysis system. This system requires a highly available relational database with an initial storage capacity of 8 TB. As a requirement, you predict that the amount of data will increase by 10 GB daily. In addition, parallel processing is required for data processing in order to handle this expected traffic volume.

Choose the best service that meets this requirement.

Options:

- A. Dynamo DB
- B. RDS
- C. Aurora
- D. Redshift

Answer: D

Explanation

Option 4 is the correct answer. Redshift is the best database for business analysis systems. Redshift is capable of big data storage and parallel query analysis processing to meet your requirements. Redshift is a petabyte-scale, relational database-type ,data warehouse service that is fully managed in the cloud. Redshift distributes table rows to compute nodes so you can process data in parallel. By choosing the appropriate distribution key for each table, you can optimize the distribution of data, distribute the workload, and minimize the movement of data between nodes.

Option 1 is incorrect. DynamoDB is a NoSQL database and does not meet the requirements of a highly available relational database.

Option 2 is incorrect. RDS is a relational database, but it cannot be used as a business analysis system. RDS can parallelize the read process by configuring a read replica. However, data analysis itself cannot be processed in parallel.

Option 3 is incorrect. Aurora MySQL can parallelize part of data-intensive query processing and computational processing. However, considering the requirements of a business analysis system, Redshift is more suitable than Aurora, so that ↑ the priority in this scenario.

Question 2:

Your company is trying to build a BI (business intelligence) system using AWS Redshift. As the Solutions Architect, you are required to use Redshift clusters in a cost-effective manner.

Which of the options will help to meet this requirement?

Options:

- A. Removing unnecessary snapshot settings
- B. Not use VPC enhanced routing
- C. Using Spot instances in your cluster
- D. Removing unnecessary CloudWatch metric settings.

Answer: A

Explanation

Redshift offers free storage for snapshots, but you'll be charged if you run out of storage. For this reason, you will be charged when the free snapshot space reaches the upper limit. To avoid this, you should save automatic snapshots and delete manual snapshots that you no longer need. You could do this by reducing the retention period. Therefore, option 1 is the correct answer.

Option 2 is incorrect. With enhanced VPC routing in Amazon Redshift, Amazon Redshift forces all COPY and UNLOAD traffic between your cluster and data repository to go through your Amazon VPC. The presence or absence of this setting does not affect the cost.

Option 3 is incorrect. If you use Spot Instances instead of On-Demand Instances, the process may be stopped in the middle of running, so this is an inappropriate setting.

Reserved Instances are available on Amazon Redshift. Knowing this, you could avoid the spot instance stoppage risks and save up to 75% (vs. on-demand pricing) by signing a one-year or three-year contract.

Option 4 is incorrect. CloudWatch metrics are free to use, but you'll be charged for custom metrics. Deleting unnecessary CloudWatch metric settings is not appropriate because it does not stop any additional charges.

Question 22:

An IT company has built a solution wherein a Redshift cluster writes data to an Amazon S3 bucket belonging to a different AWS account. However, it is found that the files created in the S3 bucket using the UNLOAD command from the Redshift cluster are not even accessible to the S3 bucket owner.

What could be the reason for this denial of permission for the bucket owner?

- A• When objects are uploaded to S3 bucket from a different AWS account, the S3 bucket owner will get implicit permissions to access these objects. This issue seems to be due to an upload error that can be fixed by providing manual access from AWS console
- B• The owner of an S3 bucket has implicit access to all objects in his bucket. Permissions are set on objects after they are completely copied to the target location. Since the owner is unable to access the uploaded files, the write operation may be still in progress
- C• When two different AWS accounts are accessing an S3 bucket, both the accounts must share the bucket policies. An erroneous policy can lead to such permission failures
- D• By default, an S3 object is owned by the AWS account that uploaded it. So the S3 bucket owner will not implicitly have access to the objects written by the Redshift cluster

Answer: D

Explanation

Correct option:

By default, an S3 object is owned by the AWS account that uploaded it. So the S3 bucket owner will not implicitly have access to the objects written by Redshift cluster - By default, an S3 object is owned by the AWS account that uploaded it. This is true even when the bucket is owned by another account. Because the Amazon Redshift data files from the UNLOAD command were put into your bucket by another account, you (the bucket owner) don't have default permission to access those files.

To get access to the data files, an AWS Identity and Access Management (IAM) role with cross-account permissions must run the UNLOAD command again. Follow these steps to set up the Amazon Redshift cluster with cross-account permissions to the bucket:

1. From the account of the S3 bucket, create an IAM role (Bucket Role) with permissions to the bucket.
2. From the account of the Amazon Redshift cluster, create another IAM role (Cluster Role) with permissions to assume the Bucket Role.
3. Update the Bucket Role to grant bucket access and create a trust relationship with the Cluster Role.
4. From the Amazon Redshift cluster, run the UNLOAD command using the Cluster Role and Bucket Role.

This solution doesn't apply to Amazon Redshift clusters or S3 buckets that use server-side encryption with AWS Key Management

Service (AWS KMS).**Incorrect options:**

When objects are uploaded to S3 bucket from a different AWS account, the S3 bucket owner will get implicit permissions to access these objects. This issue seems to be due to an upload error that can be fixed by providing manual access from AWS console - By default, an S3 object is owned by the AWS account that uploaded it. So, the bucket owner will not have any default permissions on the objects. Therefore, this option is incorrect.

The owner of an S3 bucket has implicit access to all objects in his bucket. Permissions are set on objects after they are completely copied to the target location. Since the owner is unable to access the uploaded files, the write operation may be still in progress - This is an incorrect statement, given only as a distractor.

When two different AWS accounts are accessing an S3 bucket, both the accounts must share the bucket policies. An erroneous policy can lead to such permission failures - This is an incorrect statement, given only as a distractor.

47. Aurora**Question 1:**

One company plans to migrate its PostgreSQL database to AWS. As a Solutions Architect, you have been entrusted with selecting the best database. The requirements are :

The database needs to be a standard database that performs SQL processing for business purposes.

The amount of data exceeds 15TB, and the amount of transactions per day requires a large amount of processing ability, exceeding 10,000 accesses.

You are also required to configure replicas for automatic backup to increase availability.

Choose a service that meets this requirement.

Options:

- A. PostgreSQL RDS
- B. DynamoDB
- C. Configure PostgreSQL on EC2 instance
- D. Aurora

Answer: D

Explanation

Option 4 is the correct answer. Amazon Aurora is a MySQL and PostgreSQL compatible relational database for the cloud that combines the performance and availability of traditional databases with the simplicity and cost efficiency of open source databases.

In this scenario, the amount of data is over 15TB and the daily transaction volume is over 10,000 accesses.

Options 1 and 3 are incorrect. RDS and EC2 instance-based PostgreSQL are not enough to meet this transaction volume, and the correct answer is to choose Aurora, which has higher performance than RDS PostgreSQL.

Option 2 is incorrect. Since DynamoDB is a NoSQL database, it does not meet the requirements of this case. Amazon Aurora is up to 5 times faster than a standard MySQL database and up to 3 times faster than a standard PostgreSQL database. It also offers the same security, availability, and reliability as a commercial database at one-tenth the cost. Amazon Aurora is a fully managed service with RDS that automates time-consuming administrative tasks such as hardware provisioning, database setup, patching, and backup.

Question 2:

An insurance company has a web application that serves users in the United Kingdom and Australia. The application includes a database tier using a MySQL database hosted in eu-west-2. The web tier runs from eu-west-2 and ap-southeast-2. Amazon Route 53 geoproximity routing is used to direct users to the closest web tier. It has been noted that Australian users receive slow response times to queries.

Which changes should be made to the database tier to improve performance?

Options:

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

D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2

Answer: D

Explanation

The issue here is latency with read queries being directed from Australia to UK which is great physical distance. A solution is required for improving read performance in Australia.

An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only, secondary AWS Regions. Aurora replicates data to the secondary AWS Regions with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS Region.

This solution will provide better performance for users in the Australia Region for queries. Writes must still take place in the UK Region but read performance will be greatly improved.

CORRECT: “Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2” is the correct answer.

INCORRECT: “Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region” is incorrect. The database is located in UK. If the database is migrated to Australia then the reverse problem will occur. Multi-AZ does not assist with improving query performance across Regions.

INCORRECT: “Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions” is incorrect as a relational database running on MySQL is unlikely to be compatible with DynamoDB.

INCORRECT: “Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance” is incorrect as you can only put ALBs in front of the web tier, not the DB tier.

Question 3:

A company runs a web application that serves weather updates. The application runs on a fleet of Amazon EC2 instances in a Multi-AZ Auto scaling group behind an Application Load Balancer (ALB). The instances store data in an Amazon Aurora database. A solutions architect needs to make the application more resilient to sporadic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO.)

Options:

- A. Add an Amazon CloudFront distribution in front of ALB
- B. Add an AWS WAF in front of ALB
- C. Add an AWS Global Accelerator endpoint
- D. Add Amazon Aurora Replicas
- E. Add an AWS Transit Gateway to the AZs

Answer: A & D

Explanation

The architecture is already highly resilient but may be subject to performance degradation if there are sudden increases in request rates. To resolve this situation Amazon Aurora Read Replicas can be used to serve read traffic which offloads requests from the main database. On the frontend an Amazon CloudFront distribution can be placed in front of the ALB and this will cache content for better performance and also offloads requests from the backend.

CORRECT: “Add Amazon Aurora Replicas” is the correct answer.

CORRECT: “Add an Amazon CloudFront distribution in front of the ALB” is the correct answer.

INCORRECT: “Add an AWS WAF in front of the ALB” is incorrect. A web application firewall protects applications from malicious attacks. It does not improve performance.

INCORRECT: “Add an AWS Transit Gateway to the Availability Zones” is incorrect as this is used to connect on-premises networks to VPCs.

INCORRECT: “Add an AWS Global Accelerator endpoint” is incorrect as this service is used for directing users to different instances of the application in different regions based on latency.

Question 4:

A financial services company has a web application with an application tier running in the U.S and Europe. The database tier consists of a MySQL database running on Amazon EC2 in us-west-1. Users are directed to the closest application tier using Route 53 latency-based routing. The users in Europe have reported poor performance when running queries.

Which changes should a Solutions Architect make to the database tier to improve performance?

Options:

- A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions

- B. Create an Amazon RDS Read Replica in one of the European regions. Configure the application tier in Europe to use the read replica for queries
- C. Migrate the database to Amazon RedShift. Use AWS DMS to synchronize data. Configure applications to use the RedShift data warehouse for queries
- D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure the application tier in Europe to use the local reader endpoint

Answer: D

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.

A global database can be configured in the European region and then the application tier in Europe will need to be configured to use the local database for reads/queries.

CORRECT: “Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure the application tier in Europe to use the local reader endpoint” is the correct answer.

INCORRECT: “Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions” is incorrect. You cannot configure a multi-AZ DB instance to run in another Region, it must be in the same Region but in a different Availability Zone.

INCORRECT: “Migrate the database to Amazon RedShift. Use AWS DMS to synchronize data. Configure applications to use the RedShift data warehouse for queries” is incorrect. RedShift is a data warehouse and used for running analytics queries on data that is exported from transactional database systems. It should not be used to reduce latency for users of a database, and is not a live copy of the data.

INCORRECT: “Create an Amazon RDS Read Replica in one of the European regions. Configure the application tier in Europe to use the read replica for queries” is incorrect. You cannot create an RDS Read Replica of a database that is running on Amazon EC2. You can only create read replicas of databases running on Amazon RDS.

Question 5:

The flagship application for a gaming company connects to an Amazon Aurora database and the entire technology stack is currently deployed in the United States. Now, the company has plans to expand to Europe and Asia for its operations. It needs the games table to be accessible globally but needs the users and games_played tables to be regional only.

How would you implement this with minimal application refactoring?

Options:

- A. Use a DynamoDB global table for the games table and use Amazon Aurora for the users and games_played tables
- B. Use an Amazon Aurora Global Database for the games table and use DynamoDB tables for the users and games_played tables
- C. Use an Amazon Aurora Global Database for the games table and use Amazon Aurora for the users and games_played tables
- D. Use a DynamoDB global table for the games table and use DynamoDB tables for the users and games_played tables

Answer: C

Explanation

Correct option:

Use an Amazon Aurora Global Database for the games table and use Amazon Aurora for the users and games_played tables

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. Aurora is not an in-memory database.

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. Amazon Aurora Global Database is the correct choice for the given use-case.

For the given use-case, we, therefore, need to have two Aurora clusters, one for the global table (games table) and the other one for the local tables (users and games_played tables).

Incorrect options:

Use an Amazon Aurora Global Database for the games table and use DynamoDB tables for the users and games_played tables

Use a DynamoDB global table for the games table and use Amazon Aurora for the users and games_played tables

Use a DynamoDB global table for the games table and use DynamoDB tables for the users and games_played tables

Here, we want minimal application refactoring. DynamoDB and Aurora have a completely different API, due to Aurora being SQL and DynamoDB being NoSQL. So all three options are incorrect, as they have DynamoDB as one of the components.

Question 6:

A gaming company uses Amazon Aurora as its primary database service. The company has now deployed 5 multi-AZ read replicas to increase the read throughput and for use as failover target. The replicas have been assigned the following failover priority tiers and corresponding sizes are given in parentheses: tier-1 (16TB), tier-1 (32TB), tier-10 (16TB), tier-15 (16TB), tier-15 (32TB).

In the event of a failover, Amazon RDS will promote which of the following read replicas?

Options:

- A. Tier-1 (32TB)
- B. Tier-1 (16TB)
- C. Tier-15 (32TB)
- D. Tier-10 (16TB)

Answer: A

Explanation

Correct option:

Tier-1 (32TB)

Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. It delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across three Availability Zones (AZs).

For Amazon Aurora, each Read Replica is associated with a priority tier (0-15). In the event of a failover, Amazon Aurora will promote the Read Replica that has the highest priority (the lowest numbered tier). If two or more Aurora Replicas share the same priority, then Amazon RDS promotes the replica that is largest in size. If two or more Aurora Replicas share the same priority and size, then Amazon Aurora promotes an arbitrary replica in the same promotion tier.

Therefore, for this problem statement, the Tier-1 (32TB) replica will be promoted.

Incorrect options:

- Tier-15 (32TB)
- Tier-1 (16TB)
- Tier-10 (16TB)

Given the failover rules discussed earlier in the explanation, these three options are incorrect.

Question 7:

A company manages a multi-tier social media application that runs on EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. As a solutions architect, you have been tasked to make the application more resilient to periodic spikes in request rates.

Which of the following solutions would you recommend for the given use-case? (Select two)

Options:

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

Answer: D & E

Explanation

Correct options:

You can use Aurora replicas and CloudFront distribution to make the application more resilient to spikes in request rates.

Use Aurora Replica

Aurora Replicas have two main purposes. You can issue queries to them to scale the read operations for your application. You typically do so by connecting to the reader endpoint of the cluster. That way, Aurora can spread the load for read-only connections across as many Aurora Replicas as you have in the cluster. Aurora Replicas also help to increase availability. If the writer instance in a cluster becomes unavailable, Aurora automatically promotes one of the reader instances to take its place as the new writer. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans

Use CloudFront distribution in front of the Application Load Balancer

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront points of presence (POPs) (edge locations) make sure that popular content can be served quickly to your viewers. CloudFront also has regional edge caches that bring more of your content closer to your viewers, even when the content is not popular enough to stay at a POP, to help improve performance for that content.

CloudFront offers an origin failover feature to help support your data resiliency needs. CloudFront is a global service that delivers your content through a worldwide network of data centers called edge locations or points of presence (POPs). If your content is not already cached in an edge location, CloudFront retrieves it from an origin that you've identified as the source for the definitive version of the content.

Incorrect options:

- * Use AWS Shield* - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency. There are two tiers of AWS Shield - Standard and Advanced. Shield cannot be used to improve application resiliency to handle spikes in traffic.

Use AWS Global Accelerator - AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Since CloudFront is better for improving application resiliency to handle spikes in traffic, so this option is ruled out.

Use AWS Direct Connect - AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC. Direct Connect cannot be used to improve application resiliency to handle spikes in traffic.

Question 4: Skipped

A company is developing a healthcare application that cannot afford any downtime for database write operations. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution using Amazon Aurora.

Which of the following options would you recommend?

- Set up an Aurora multi-master DB cluster (Correct)
- Set up an Aurora provisioned DB cluster
- Set up an Aurora Global Database cluster
- Set up an Aurora serverless DB cluster

Explanation

Correct option:

Set up an Aurora multi-master DB cluster

In a multi-master cluster, all DB instances can perform write operations. There isn't any failover when a writer DB instance becomes unavailable, because another writer DB instance is immediately available to take over the work of the failed instance. AWS refers to this type of availability as continuous availability, to distinguish it from the high availability (with brief downtime during failover) offered by a single-master cluster. For applications where you can't afford even brief downtime for database write operations, a multi-master cluster can help to avoid an outage when a writer instance becomes unavailable. The multi-master cluster doesn't use the failover mechanism, because it doesn't need to promote another DB instance to have read/write capability.

Incorrect options:

Set up an Aurora serverless DB cluster

Set up an Aurora provisioned DB cluster

Set up an Aurora Global Database cluster

These three options represent Aurora single-master clusters. In a single-master cluster, a single DB instance performs all write operations and any other DB instances are read-only. If the writer DB instance becomes unavailable, a failover mechanism promotes one of the read-only instances to be the new writer. As there is a brief downtime during this failover, these three options are incorrect for the given use case.

48. Elasticache**49. Database Migration Services (DMS)**

Question 1:

The database tier of a web application is running on a Windows server on-premises. The database is a Microsoft SQL Server database. The application owner would like to migrate the database to an Amazon RDS instance.

How can the migration be executed with minimal administrative effort and downtime?

Options:

- A. Use the AWS Server Migration Service (SMS) to migrate the server to Amazon EC2. Use AWS Database Migration Service (DMS) to migrate the database to RDS
- B. Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS
- C. Use AWS DataSync to migrate the data from the database to Amazon S3. Use AWS Database Migration Service (DMS) to migrate the database to RDS
- D. Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS. Use the Schema Conversion Tool (SCT) to enable conversion from Microsoft SQL Server to Amazon RDS

Answer: B

Explanation

You can directly migrate Microsoft SQL Server from an on-premises server into Amazon RDS using the Microsoft SQL Server database engine. This can be achieved using the native Microsoft SQL Server tools, or using AWS DMS.

CORRECT: “Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS” is the correct answer.

INCORRECT: “Use the AWS Server Migration Service (SMS) to migrate the server to Amazon EC2. Use AWS Database Migration Service (DMS) to migrate the database to RDS” is incorrect. You do not need to use the AWS SMS service to migrate the server into EC2 first. You can directly migrate the database online with minimal downtime.

INCORRECT: “Use AWS DataSync to migrate the data from the database to Amazon S3. Use AWS Database Migration Service (DMS) to migrate the database to RDS” is incorrect. AWS DataSync is used for migrating data, not databases.

INCORRECT: “Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS. Use the Schema Conversion Tool (SCT) to enable conversion from Microsoft SQL Server to Amazon RDS” is incorrect. You do not need to use the SCT as you are migrating into the same destination database engine (RDS is just the platform).

50. Caching Strategies**51. EMR****52. Directory Service****53. IAM Policies****54. Resource Access Manager (RAM)****55. Single Sign-On****56. Route 53 – Domain Name Server (DNS)****57. Route 53 – Register a Domain Name Lab****58. Route 53 Routing Policies**

Question 1:

The development team at an e-commerce startup has set up multiple microservices running on EC2 instances under an Application Load Balancer. The team wants to route traffic to multiple back-end services based on the URL path of the HTTP header. So it wants requests for www.example.com/orders to go to a specific microservice and requests for www.example.com/products to go to another microservice.

Which of the following features of Application Load Balancers can be used for this use-case?

Options:

- A. Path-based Routing
- B. HTTP header-based routing
- C. Query string parameter-based routing
- D. Host-based routing

Answer: A

Explanation

Correct option:

Path-based Routing

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.

If your application is composed of several individual services, an Application Load Balancer can route a request to a service based on the content of the request. Here are the different types –

Host-based Routing:

You can route a client request based on the Host field of the HTTP header allowing you to route to multiple domains from the same load balancer.

Path-based Routing:

You can route a client request based on the URL path of the HTTP header.

HTTP header-based routing:

You can route a client request based on the value of any standard or custom HTTP header.

HTTP method-based routing:

You can route a client request based on any standard or custom HTTP method.

Query string parameter-based routing:

You can route a client request based on the query string or query parameters.

Source IP address CIDR-based routing:

You can route a client request based on source IP address CIDR from where the request originates.

Path-based Routing Overview:

You can use path conditions to define rules that route requests based on the URL in the request (also known as path-based routing).

The path pattern is applied only to the path of the URL, not to its query parameters.

Incorrect options:

Query string parameter-based routing

HTTP header-based routing

Host-based Routing

As mentioned earlier in the explanation, none of these three types of routing support requests based on the URL path of the HTTP header. Hence these three are incorrect.

59. Route 53 Simple Routing Policy

Question 1:

As a Solutions Architect, you are building a WEB application configured using two EC2 instances. You would like to configure it to randomly route to each server using Route53.

Choose a routing policy that meets this requirement.

Options:

- A. Simple routing policy
- B. Weighted routing policy
- C. Latency routing policy
- D. Failover routing policy

Answer: A

Explanation

Option 1 is the correct answer. Simple routing is used when a domain has a single resource that performs a specific function. Simple routing routes traffic randomly across multiple instances. Therefore, simple routing is sufficient for random routing.

Option 2 is incorrect. Weighted routing allows you to associate multiple resources with a single domain name (example.com) or

subdomain name (acme.example.com) and set the routing weight for each resource. It is used to route traffic to multiple resources in proportions that you specify.

Option 3 is incorrect. Latency routing can improve user performance by routing requests to the AWS Region with the lowest network latency when you are hosting your application in multiple AWS Regions.

Option 4 is incorrect. Failover routing allows you to stop routing to anomalous resources and route traffic to healthy resources.

60. Route 53 Weighted Routing Policy

61. Route 53 Latency Routing Policy

62. Route 53 Failover Routing Policy

Question 1:

As a Solutions Architect, you are building an application that uses AWS. The application has primary and secondary configurations across two regions, each utilizing ELB, Auto scaling, and EC2 instances.

Choose the best Route 53 routing policy if your primary infrastructure goes down.

Options:

- A. Weighted routing
- B. Simple routing
- C. Multi-value answer routing
- D. Failover routing

Answer: D

Explanation

You can use the Failover routing policy to create an active-passive failover configuration. You can create primary and secondary failover records of the same name and type and associate health checks with each to achieve a cross-region failover configuration. Option 4 is the correct answer.

Amazon Route 53 Health Check monitors the health and performance of web applications, web servers, and other resources. Route 53 monitors performance in one of the following ways:

1. Health check for specified resources such as web servers
2. Status of other health checks such as ELB
3. Amazon CloudWatch Alarm Status

Option 1 is incorrect. Weighted routing allows you to route traffic to multiple resources with a custom ratio.

Option 2 is incorrect. Simple routing is used when a domain has a single resource that performs a particular function. For example, a single web server that serves content to a website.

Option 3 is incorrect. Multi-value answer routing is used when Route 53 responds to DNS queries with up to eight randomly selected healthy records.

Question 2:

A company has deployed a new website on Amazon EC2 instances behind an Application Load Balancer (ALB). Amazon Route 53 is used for the DNS service. The company has asked a Solutions Architect to create a backup website with support contact details that users will be directed to automatically if the primary website is down.

How should the Solutions Architect deploy this solution cost-effectively?

Options:

- A. Deploy the backup website on EC2 and ALB in another Region and use Route 53 health checks for failover routing
- B. Configure a static website using Amazon S3 and create a Route 53 weighted routing policy" is incorrect
- C. Configure a static website using Amazon S3 and create a Route 53 failover routing policy
- D. Create the backup website on EC2 and ALB in another Region and create an AWS Global Accelerator endpoint

Answer: C

Explanation

The most cost-effective solution is to create a static website using an Amazon S3 bucket and then use a failover policy in Amazon Route 53. With a failover routing policy users will be directed to the main website as long as it is responsive to health checks successfully.

If the main website fails to respond to health checks (its down), Route 53 will begin to direct users to the backup website running on the Amazon S3 bucket. It's important to set the TTL on the Route 53 records appropriately to ensure that users resolve the failover address within a short time.

CORRECT: “Configure a static website using Amazon S3 and create a Route 53 failover routing policy” is the correct answer.

INCORRECT: “Configure a static website using Amazon S3 and create a Route 53 weighted routing policy” is incorrect. Weighted routing is used when you want to send a percentage of traffic between multiple endpoints. In this case all traffic should go to the primary until it fails, then all should go to the backup.

INCORRECT: “Deploy the backup website on EC2 and ALB in another Region and use Route 53 health checks for failover routing” is incorrect. This is not a cost-effective solution for the backup website. It can be implemented using Route 53 failover routing which uses health checks but would be an expensive option.

INCORRECT: “Create the backup website on EC2 and ALB in another Region and create an AWS Global Accelerator endpoint” is incorrect. Global Accelerator is used for performance as it directs traffic to the nearest healthy endpoint. It is not useful for failover in this scenario and is also a very expensive solution.

Question 11: Skipped

A manufacturing company receives unreliable service from its data center provider because the company is located in an area prone to natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failover environment on AWS in case the on-premises data center fails. The company runs web servers that connect to external vendors. The data available on AWS and on-premises must be uniform.

Which of the following solutions would have the LEAST amount of downtime?

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

Explanation

Correct option:

Set up a Route 53 failover record. Run application servers on EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to S3

If you have multiple resources that perform the same function, you can configure DNS failover so that Route 53 will route your traffic from an unhealthy resource to a healthy resource.

Elastic Load Balancing is used to automatically distribute your incoming application traffic across all the EC2 instances that you are running. You can use Elastic Load Balancing to manage incoming requests by optimally routing traffic so that no one instance is overwhelmed. Your load balancer acts as a single point of contact for all incoming web traffic to your Auto Scaling group.

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. It provides low-latency performance by caching frequently accessed data on-premises while storing data securely and durably in Amazon cloud storage services. Storage Gateway optimizes data transfer to AWS by sending only changed data and compressing data. Storage Gateway also integrates natively with Amazon S3 cloud storage which makes your data available for in-cloud processing.

Incorrect options:

Set up a Route 53 failover record. Execute an AWS CloudFormation template from a script to provision EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to S3

Set up a Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to S3. Set up an AWS Direct Connect connection between a VPC and the data center

Set up a Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer ↑

AWS CloudFormation is a convenient provisioning mechanism for a broad range of AWS and third-party resources. It supports the

infrastructure needs of many different types of applications such as existing enterprise applications, legacy applications, applications built using a variety of AWS resources, and container-based solutions.

These three options involve CloudFormation as part of the solution. Now, CloudFormation takes time to provision the resources and hence is not the right solution when LEAST amount of downtime is mandated for the given use case. Therefore, these options are not the right fit for the given requirement.

63. Route 53 Geolocation Routing Policy

Question 1:

Your company hosts many infrastructures in the Tokyo region. As a Solutions Architect, you are trying to replicate these infrastructure configurations on the Singapore and Sydney regions to extend your application. Optimal language selection and routing control is required to satisfy users close to the region.

What do you need to do to achieve optimal language selection for your users and ELB routing control?

Options:

- A. Set up geo-location routing on Route53
- B. Perform load balancing for all regions using NLB
- C. Configure low latency routing on Route53
- D. Perform load balancing for all regions using ALB

Answer: A

Explanation

Option 1 is the correct answer. With geo-location routing, resources are selected to handle traffic based on the user's geographic location. As a result, language display and traffic processing will be easy to implement.

When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries:

Simple routing policy – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.

Failover routing policy – Use this when you want to configure active-passive failover.

Geo-location routing policy – Use when you want to route traffic based on the location of your users.

Geo-proximity routing policy – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.

Latency routing policy – Use when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.

Multi-value answer routing policy – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.

Weighted routing policy – Use to route traffic to multiple resources in proportions that you choose.

Question 2:

A company hosts an application on Amazon EC2 instances behind Application Load Balancers in several AWS Regions. Distribution rights for the content require that users in different geographies must be served content from specific regions.

Which configuration meets these requirements?

Options:

- A. Configure Amazon CloudFront with multiple origins and AWS WAF
- B. Create Amazon Route 53 records with a geoproximity routing policy
- C. Create Amazon Route 53 records with a geolocation routing policy
- D. Configure Application Load Balancers with multi-Region routing

Answer: C

Explanation

To protect the distribution rights of the content and ensure that users are directed to the appropriate AWS Region based on the location of the user, the geolocation routing policy can be used with Amazon Route 53.

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from.

When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution

rights.

CORRECT: “Create Amazon Route 53 records with a geolocation routing policy” is the correct answer.

INCORRECT: “Create Amazon Route 53 records with a geoproximity routing policy” is incorrect. Use this routing policy when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.

INCORRECT: “Configure Amazon CloudFront with multiple origins and AWS WAF” is incorrect. AWS WAF protects against web exploits but will not assist with directing users to different content (from different origins).

INCORRECT: “Configure Application Load Balancers with multi-Region routing” is incorrect. There is no such thing as multi-Region routing for ALBs.

Question 03:

One of the biggest football leagues in Europe has granted the distribution rights for live streaming its matches in the US to a silicon valley based streaming services company. As per the terms of distribution, the company must make sure that only users from the US are able to live stream the matches on their platform. Users from other countries in the world must be denied access to these live-streamed matches.

Which of the following options would allow the company to enforce these streaming restrictions? (Select two)

- A. Use Route 53 based geolocation routing policy to restrict distribution of content to only the locations in which you have distribution rights
- B. Use Route 53 based latency routing policy to restrict distribution of content to only the locations in which you have distribution rights
- C. Use Route 53 based weighted routing policy to restrict distribution of content to only the locations in which you have distribution rights
- D. Use georestriction to prevent users in specific geographic locations from accessing content that you’re distributing through a CloudFront web distribution
- E. Use Route 53 based failover routing policy to restrict distribution of content to only the locations in which you have distribution rights

Answer: A & D

Explanation

Correct options:

Use Route 53 based geolocation routing policy to restrict distribution of content to only the locations in which you have distribution rights

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region. You can also use geolocation routing to restrict the distribution of content to only the locations in which you have distribution rights.

Use georestriction to prevent users in specific geographic locations from accessing content that you’re distributing through a CloudFront web distribution

You can use georestriction, also known as geo-blocking, to prevent users in specific geographic locations from accessing content that you’re distributing through a CloudFront web distribution. When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following: Allow your users to access your content only if they’re in one of the countries on a whitelist of approved countries. Prevent your users from accessing your content if they’re in one of the countries on a blacklist of banned countries. So this option is also correct.

Incorrect options:

Use Route 53 based latency routing policy to restrict distribution of content to only the locations in which you have distribution rights – Use latency based routing when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the lowest latency. To use latency-based routing, you create latency records for your resources in multiple AWS Regions. When Route 53 receives a DNS query for your domain or subdomain (example.com or acme.example.com), it determines which AWS Regions you’ve created latency records for, determines which region gives the user the lowest latency, and then selects a latency record for that region. Route 53 responds with the value from the selected record, such as the IP address for a web server.

Use Route 53 based weighted routing policy to restrict distribution of content to only the locations in which you have distribution rights – Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes,

including load balancing and testing new versions of the software.

Use Route 53 based failover routing policy to restrict distribution of content to only the locations in which you have distribution rights – Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. The primary and secondary records can route traffic to anything from an Amazon S3 bucket that is configured as a website to a complex tree of records

Weighted routing or failover routing or latency routing cannot be used to restrict the distribution of content to only the locations in which you have distribution rights. So all three options above are incorrect.

64. Route 53 Geoproximity Routing Policy (Traffic Flow Only)

65. Route 53 Multivalue Answer

66. VPCs

Question 1: Company-A operates a business system that uses AWS resources such as VPC. Recently, the management of company-A has acquired company-B, and you, as a solution architect, have been put in charge of IT integration between these two companies. Company-B also has its own set of resources that are hosted on AWS. The requirement is to allow AWS resources in the company-A's VPC to access AWS resources in Company B's VPC. What action do you need to take to meet this requirement?

Options:

- A. Install a NAT instance in each VPC and connect between VPCs
- B. Install a NAT gateway in each VPC and connect between VPCs
- C. Connect VPC's through the organization settings of AWS Organizations
- D. Connect VPCs by VPC peering

Answer: D

Explanation:

A VPC peering connection allows you to network between two VPCs for private traffic routing. This allows instances configured in two VPCs to communicate with each other as if they were in the same network. Therefore, option 4 is the correct answer. A VPC peering connection is a network connection that allows you to route traffic between VPCs using a private IPv4 or IPv6 address. This allows instances in both VPCs to communicate with each other as if they were in the same network. VPC peering connections are work for connections between VPCs from one AWS account, or even between multiple AWS accounts, regardless of region.

Options 1 and 2 are incorrect. A NAT instance or NAT gateway is a gateway that allows an instance in a private subnet to reply to the Internet. This is done by translating a private IP address into a public IP address. This function, however, has nothing to do with the connection between VPCs.

Option 3 is incorrect. AWS Organizations is a feature that enables integrated management of multiple AWS accounts. You can use this to share VPCs between accounts, but it will not be used to connect between VPCs.

Question 2:

As a Solutions Architect, you are building an application on AWS. This application is setting up an EC2 instance with a public IP in the subnet of a VPC. It appears you couldn't connect to your EC2 instance over the internet. The security group seems to be set up correctly.

What should I do to connect to an EC2 instance from the internet?

Options:

- A. Set the correct route in the route table
- B. Set Elastic IP to your EC2 instance
- C. Set the secondary IP address to your EC2 instance
- D. Set up a NAT gateway

Answer: A

Explanation

In order for this EC2 instance to be accessible from the Internet, the security groups and network ACLs must be properly configured and the subnet's route table in place must have an entry to the Internet gateway. Therefore, option 1 is the correct answer.

Option 2 is incorrect. Elastic IP is not required to access from the internet.

Option 3 is incorrect. A secondary IP is not required to access from the internet.

Option 4 is incorrect. The NAT gateway is used to access an EC2 instance in the private subnet, not public.

Question 3:

A company has two accounts for perform testing and each account has a single VPC: VPC-TEST1 and VPC-TEST2. The operations team require a method of securely copying files between Amazon EC2 instances in these VPCs. The connectivity should not have any single points of failure or bandwidth constraints.

Which solution should a Solutions Architect recommend?

Options:

- A. Attach a virtual private gateway to VPC-TEST1 and VPC-TEST2 and enable routing
- B. Create a VPC peering connection between VPC-TEST1 and VPC-TEST2
- C. Create a VPC gateway endpoint for each EC2 instance and update route tables
- D. Attach a Direct Connect gateway to VPC-TEST1 and VPC-TEST2 and enable routing

Answer: B

Explanation

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

You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

CORRECT: “Create a VPC peering connection between VPC-TEST1 and VPC-TEST2” is the correct answer.

INCORRECT: “Create a VPC gateway endpoint for each EC2 instance and update route tables” is incorrect. You cannot create VPC gateway endpoints for Amazon EC2 instances. These are used with DynamoDB and S3 only.

INCORRECT: “Attach a virtual private gateway to VPC-TEST1 and VPC-TEST2 and enable routing” is incorrect. You cannot create an AWS Managed VPN connection between two VPCs.

INCORRECT: “Attach a Direct Connect gateway to VPC-TEST1 and VPC-TEST2 and enable routing” is incorrect. Direct Connect gateway is used to connect a Direct Connect connection to multiple VPCs, it is not useful in this scenario as there is no Direct Connect connection.

Question 4:

The sourcing team at the US headquarters of a global e-commerce company is preparing a spreadsheet of the new product catalog. The spreadsheet is saved on an EFS file system created in us-east-1 region. The sourcing team counterparts from other AWS regions such as Asia Pacific and Europe also want to collaborate on this spreadsheet.

As a solutions architect, what is your recommendation to enable this collaboration with the LEAST amount of operational overhead?

Options

- A. The spreadsheet will have to be copied in Amazon S3 which can then be accessed from any AWS region
- B. The spreadsheet data will have to be moved into an RDS MySQL database which can then be accessed from any AWS region
- C. The spreadsheet on the EFS file system can be accessed in other AWS regions by using an inter-region VPC peering connection
- D. The spreadsheet will have to be copied into EFS file systems of other AWS regions as EFS is a regional service and it does not allow access from other AWS regions

Answer: C

Explanation

Correct option:

The spreadsheet on the EFS file system can be accessed in other AWS regions by using an inter-region VPC peering connection

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources.

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

You can connect to Amazon EFS file systems from EC2 instances in other AWS regions using an inter-region VPC peering connection, and from on-premises servers using an AWS VPN connection. So this is the correct option.

Incorrect options:

The spreadsheet will have to be copied in Amazon S3 which can then be accessed from any AWS region

The spreadsheet data will have to be moved into an RDS MySQL database which can then be accessed from any AWS region

Copying the spreadsheet into S3 or RDS database is not the correct solution as it involves a lot of operational overhead. For RDS, one would need to write custom code to replicate the spreadsheet functionality running off of the database. S3 does not allow in-place edit of an object. Additionally, it's also not POSIX compliant. So one would need to develop a custom application to "simulate in-place edits" to support collaboration as per the use-case. So both these options are ruled out.

The spreadsheet will have to be copied into EFS file systems of other AWS regions as EFS is a regional service and it does not allow access from other AWS regions – Creating copies of the spreadsheet into EFS file systems of other AWS regions would mean no collaboration would be possible between the teams. In this case, each team would work on "its own file" instead of a single file accessed and updated by all teams. Hence this option is incorrect.

Question 7: Skipped

A systems administrator has created a private hosted zone and associated it with a Virtual Private Cloud (VPC). However, the DNS queries for the private hosted zone remain unresolved.

As a Solutions Architect, can you identify the Amazon VPC options to be configured in order to get the private hosted zone to work?

- Enable DNS hostnames and DNS resolution for private hosted zones (Correct)
- Fix the Name server (NS) record and Start Of Authority (SOA) records that may have been created with wrong configurations
- Remove any overlapping namespaces for the private and public hosted zones
- Fix conflicts between your private hosted zone and any Resolver rule that routes traffic to your network for the same domain name, as it results in ambiguity over the route to be taken

Explanation

Correct option:

Enable DNS hostnames and DNS resolution for private hosted zones – DNS hostnames and DNS resolution are required settings for private hosted zones. DNS queries for private hosted zones can be resolved by the Amazon-provided VPC DNS server only. As a result, these options must be enabled for your private hosted zone to work.

DNS hostnames: For non-default virtual private clouds that aren't created using the Amazon VPC wizard, this option is disabled by default. If you create a private hosted zone for a domain and create records in the zone without enabling DNS hostnames, private hosted zones aren't enabled. To use a private hosted zone, this option must be enabled.

DNS resolution: Private hosted zones accept DNS queries only from a VPC DNS server. The IP address of the VPC DNS server is the reserved IP address at the base of the VPC IPv4 network range plus two. Enabling DNS resolution allows you to use the VPC DNS server as a Resolver for performing DNS resolution. Keep this option disabled if you're using a custom DNS server in the DHCP Options set, and you're not using a private hosted zone.

Incorrect options:

Remove any overlapping namespaces for the private and public hosted zones – If you have private and public hosted zones that have overlapping namespaces, such as example.com and accounting.example.com, then the Resolver routes traffic based on the most specific match. It won't result in unresolved queries, hence this option is wrong.

Fix the Name server (NS) record and Start Of Authority (SOA) records that may have been created with wrong configurations – When you create a hosted zone, Amazon Route 53 automatically creates a name server (NS) record and a start of authority (SOA) record for the zone for public hosted zone. However, this issue is about the private hosted zone, hence this is an incorrect option.

Fix conflicts between your private hosted zone and any Resolver rule that routes traffic to your network for the same domain name, as it results in ambiguity over the route to be taken – If you have a private hosted zone (example.com) and a Resolver rule that routes traffic to your network for the same domain name, the Resolver rule takes precedence. It won't result in unresolved queries.

Question 27:

You have multiple AWS accounts within a single AWS Region managed by AWS Organizations and you would like to ensure all EC2 instances in all these accounts can communicate privately. Which of the following solutions provides the capability at the CHEAPEST cost?

- A• Create a VPC peering connection between all VPCs
- B• Create a VPC in an account and share one or more of its subnets with the other accounts using Resource Access Manager
- C• Create a Private Link between all the EC2 instances
- D• Create a Transit Gateway and link all the VPC in all the accounts together

Answer: B

Explanation

Correct option:

Create a VPC in an account and share one or more of its subnets with the other accounts using Resource Access Manager

AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. You can share AWS Transit Gateways, Subnets, AWS License Manager configurations, and Amazon Route 53 Resolver rules resources with RAM. RAM eliminates the need to create duplicate resources in multiple accounts, reducing the operational overhead of managing those resources in every single account you own. You can create resources centrally in a multi-account environment, and use RAM to share those resources across accounts in three simple steps: create a Resource Share, specify resources, and specify accounts. RAM is available to you at no additional charge.

The correct solution is to share the subnet(s) within a VPC using RAM. This will allow all EC2 instances to be deployed in the same VPC (although from different accounts) and easily communicate with one another.

Incorrect options:

Create a Private Link between all the EC2 instances – AWS PrivateLink simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet. AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. Private Link is a distractor in this question. Private Link is leveraged to create a private connection between an application that is fronted by an NLB in an account, and an Elastic Network Interface (ENI) in another account, without the need of VPC peering and allowing the connections between the two to remain within the AWS network.

Create a VPC peering connection between all VPCs – A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection). VPC peering connections will work, but won't efficiently scale if you add more accounts (you'll have to create many connections).

Create a Transit Gateway and link all the VPC in all the accounts together – AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. A Transit Gateway will work but will be an expensive solution. Here we want to minimize cost.

67. Build a Custom VPC

68. Network Address Translation (NAT)

Question 1:

As a Solutions Architect, you use AWS to host a database server within your company. This server should not be able to connect to the Internet unless you want to download the required database patches.

Choose an AWS service configuration that meets this requirement.

Option:

- A. Build the DB in a public subnet and allow only inbound traffic with network ACLs
- B. Build the DB in the public subnet and allow only inbound traffic in the security group
- C. Build the DB in a private subnet and allow only outbound traffic in the security group
- D. Build the DB in a private subnet and set the NAT instance in the route table

Answer: D

Explanation

To restrict internet access to your database, you need to have a DB instance in your private subnet. On top of that, the DB should only be allowed to reply to the Internet via NAT. Therefore, option 4 is the correct answer.

EC2 instances located on public subnets can send outbound traffic directly to the Internet, but EC2 instances located on private subnets cannot. Instead, instances located on the private subnet can use a Network Address Translation (NAT) gateway located on the public subnet to return traffic to the Internet side. This allows the database server to connect to the Internet through a NAT instance for software updates, but a connection to the database server from the Internet cannot be established ↑

Options 1 and 2 are incorrect. If you build the database in the public subnet, you can access it directly from the Internet, so it is

better to install it in the private subnet.

Option 3 is incorrect. After building the database in a private subnet, the security group controls inbound traffic. Security groups can restrict access to your database by allowing access only from specific EC2 instances.

Question 2:

Your company operates infrastructure located on AWS's private and public subnets. A database server is installed in the private subnet. In addition, a NAT instance is installed in the public subnet because the instance in the private subnet sends the reply traffic to the Internet side. Recently, you have discovered that your NAT instance is becoming bottlenecked.

How should you do to solve this issue?

Options:

- A. Use VPC connection for a wider bandwidth
- B. Set access settings using VPC endpoints
- C. Change the NAT instance to a NAT gateway
- D. Scale-up the NAT instance

Answer: C

Explanation

Option 3 is the correct answer. A NAT gateway is a managed service that you can use instead of a NAT instance. Since availability is guaranteed as a managed service on the AWS side, using a NAT gateway will improve the bottleneck of your current NAT instance. Scaling, such as changing the instance type of the NAT instance itself, can help, but it does not guarantee that the problem will not occur in the future. Therefore, you can easily improve performance and eliminate bottlenecks by changing your NAT instance to a NAT gateway.

Option 1 is incorrect. There is no function called VPC connection.

Option 2 is incorrect. A VPC endpoint is a communication path used to connect AWS resources from inside to outside the VPC.

Option 4 is incorrect. It is possible to deal with this by extending the NAT instance, but AWS provides a NAT gateway as a managed service, so it is more effective to use this instead.

69. Access Control List (ACL)

70. Custom VPCs and ELBs

Question 1:

A solutions architect is designing the infrastructure to run an application on Amazon EC2 instances. The application requires high availability and must dynamically scale based on demand to be cost efficient.

What should the solutions architect do to meet these requirements?

Options:

- A. Configure an Amazon CloudFront distribution in front of an Auto Scaling group to deploy instances to multiple Regions
- B. Configure an Amazon API Gateway API in front of an Auto Scaling group to deploy instances to multiple Availability Zones
- C. Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Availability Zones
- D. Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Regions

Answer: C

Explanation

The Amazon EC2-based application must be highly available and elastically scalable. Auto Scaling can provide the elasticity by dynamically launching and terminating instances based on demand. This can take place across availability zones for high availability.

Incoming connections can be distributed to the instances by using an Application Load Balancer (ALB).

CORRECT: "Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Availability Zones" is the correct answer.

INCORRECT: "Configure an Amazon API Gateway API in front of an Auto Scaling group to deploy instances to multiple Availability Zones" is incorrect as API gateway is not used for load balancing connections to Amazon EC2 instances

INCORRECT: "Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Regions"

is incorrect as you cannot launch instances in multiple Regions from a single Auto Scaling group.

INCORRECT: “Configure an Amazon CloudFront distribution in front of an Auto Scaling group to deploy instances to multiple Regions” is incorrect as you cannot launch instances in multiple Regions from a single Auto Scaling group.

Question 2:

A Solutions Architect has deployed an application on several Amazon EC2 instances across three private subnets. The application must be made accessible to internet-based clients with the least amount of administrative effort.

How can the Solutions Architect make the application available on the internet?

Options:

- A. Create an Amazon Machine Image (AMI) of the instances in the private subnet and launch new instances from the AMI in public subnets. Create an Application Load Balancer and add the public instances to the ALB
- B. Create an Application Load Balancer and associate three private subnets from the same Availability Zones as the private instances. Add the private instances to the ALB
- C. Create a NAT gateway in a public subnet. Add a route to the NAT gateway to the route tables of the three private subnets
- D. Create an Application Load Balancer and associate three public subnets from the same Availability Zones as the private instances. Add the private instances to the ALB

Answer: D

Explanation

To make the application instances accessible on the internet the Solutions Architect needs to place them behind an internet-facing Elastic Load Balancer. The way you add instances in private subnets to a public facing ELB is to add public subnets in the same AZs as the private subnets to the ELB. You can then add the instances and to the ELB and they will become targets for load balancing.

CORRECT: “Create an Application Load Balancer and associate three public subnets from the same Availability Zones as the private instances. Add the private instances to the ALB” is the correct answer.

INCORRECT: “Create an Application Load Balancer and associate three private subnets from the same Availability Zones as the private instances. Add the private instances to the ALB” is incorrect. Public subnets in the same AZs as the private subnets must be added to make this configuration work.

INCORRECT: “Create an Amazon Machine Image (AMI) of the instances in the private subnet and launch new instances from the AMI in public subnets. Create an Application Load Balancer and add the public instances to the ALB” is incorrect. There is no need to use an AMI to create new instances in a public subnet. You can add instances in private subnets to a public-facing ELB.

INCORRECT: “Create a NAT gateway in a public subnet. Add a route to the NAT gateway to the route tables of the three private subnets” is incorrect. A NAT gateway is used for outbound traffic not inbound traffic and cannot make the application available to internet-based clients.

Question 3:

A company’s web application is using multiple Amazon EC2 Linux instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure.

What should a solutions architect do to meet these requirements?

Options:

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

Answer: C

Explanation

To increase the resiliency of the application the solutions architect can use Auto Scaling groups to launch and terminate instances across multiple availability zones based on demand. An application load balancer (ALB) can be used to direct traffic to the web application running on the EC2 instances.

Lastly, the Amazon Elastic File System (EFS) can assist with increasing the resilience of the application by providing a shared file system that can be mounted by multiple EC2 instances from multiple availability zones.

CORRECT: “Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on

Amazon EFS and mount a target on each instance” is the correct answer.

INCORRECT: “Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance” is incorrect as the EBS volumes are single points of failure which are not shared with other instances.

INCORRECT: “Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance” is incorrect as instance stores are ephemeral data stores which means data is lost when powered down. Also, instance stores cannot be shared between instances.

INCORRECT: “Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)” is incorrect as there are data retrieval charges associated with this S3 tier. It is not a suitable storage tier for application files.

Question 4:

A developer has created a new Application Load Balancer but has not registered any targets with the target groups. Which of the following errors would be generated by the Load Balancer?

- A. HTTP 504: Gateway timeout
- B. HTTP 502: Bad gateway
- C. HTTP 503: Service unavailable
- D. HTTP 500: Internal server error

Answer: C

Explanation

Correct option:

HTTP 503: Service unavailable

The Load Balancer generates the HTTP 503: Service unavailable error when the target groups for the load balancer have no registered targets.

Incorrect options:

HTTP 500: Internal server error

HTTP 502: Bad gateway

HTTP 504: Gateway timeout

Question 5:

An e-commerce company is looking for a solution with high availability, as it plans to migrate its flagship application to a fleet of Amazon EC2 instances. The solution should allow for content-based routing as part of the architecture.

As a Solutions Architect, which of the following will you suggest for the company?

Options:

- A. Use a Network Load Balancer for distributing traffic to the EC2 instances spread across different Availability Zones. Configure a Private IP address to mask any failure of an instance
- B. Use an Application Load Balancer for distributing traffic to the EC2 instances spread across different Availability Zones. Configure Auto Scaling group to mask any failure of an instance
- C. Use an Auto Scaling group for distributing traffic to the EC2 instances spread across different Availability Zones. Configure an Elastic IP address to mask any failure of an instance
- D. Use an Auto Scaling group for distributing traffic to the EC2 instances spread across different Availability Zones. Configure a Public IP address to mask any failure of an instance

Answer: B

Explanation

Correct option:

Use an Application Load Balancer for distributing traffic to the EC2 instances spread across different Availability Zones. Configure Auto Scaling group to mask any failure of an instance

The Application Load Balancer (ALB) is best suited for load balancing HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers. Operating at the individual request level (Layer 7), the Application Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) based on the content of the request.

This is the correct option since the question has a specific requirement for content-based routing which can be configured via the Application Load Balancer. Different AZs provide high availability to the overall architecture and Auto Scaling will help mask any instance failures.

Incorrect options:

Use a Network Load Balancer for distributing traffic to the EC2 instances spread across different Availability Zones. Configure a Private IP address to mask any failure of an instance – Network Load Balancer cannot facilitate content-based routing so this option is incorrect.

Use an Auto Scaling group for distributing traffic to the EC2 instances spread across different Availability Zones. Configure an Elastic IP address to mask any failure of an instance

Use an Auto Scaling group for distributing traffic to the EC2 instances spread across different Availability Zones. Configure a Public IP address to mask any failure of an instance

Both these options are incorrect as you cannot use the Auto Scaling group to distribute traffic to the EC2 instances.

An Elastic IP address is a static, public, IPv4 address allocated to your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Elastic IPs do not change and remain allocated to your account until you delete them.

71. VPC Flow Logs

72. Bastions

Question 1:

Your company runs an application hosted on AWS. The application utilizes two EC2 instances in two public subnets. Only specific users in the company access the WEB server via the Internet. The other instance is set up as a database server. As a security officer, you have begun to consider improving the security of this current architecture.

Which of the following is the most secure configuration?

Options:

- A. Create a new private subnet and place a NAT instance on it
- B. Move the web server to a private subnet
- C. Move the DB server to a private subnet
- D. Migrate both servers to the new private subnet and set up a bastion server on the public subnet

Answer: D

Explanation

Option 4 is the correct answer. The most secure configuration is to migrate both the web server and the database server to a private subnet and put the NAT gateway on the public subnet. Allows access to the WEB server via the public subnet bastion server or ELB.

If the web server requires unspecified access from the internet, this web server should be on a public subnet. However, in this case, only internal users access the web server from the internal network, so we can see that this web server is limited to internal access. Therefore, it is desirable for security to install the WEB server on a private subnet.

Option 1 is incorrect. It is necessary to create a new private subnet and relocate the server. However, the need to install a NAT instance will not achieve the requirements of this scenario.

Option 2 is incorrect. Not only should the the web server move to the private subnet, but the database server should also move to the private subnet.

Option 3 is incorrect. Not only should the DB server move to the private subnet, but the WEB server should also move to the private subnet.

73. Direct Connect

Question 1:

As a Solutions Architect, you are considering migrating from your on-premises environment to AWS. The company currently holds large amounts of data in its data centers, and this on-premises environment will continue to be used. Therefore, a high performance, leased line connection of 50 Mbps is required to connect this data center to AWS.

Choose the best connection method to meet this requirement.

Options:

- A. Make a connection to your on-premises environment through VPC peering
- B. Connect to on-premises environment via VPN
- C. Make a connection to on-premises environment with AWS Direct Connect
- D. Make a connection to on-premises environment through an internet gateway

Answer: C

Explanation

AWS Direct Connect makes it easy to establish a dedicated network connection to AWS from an on-premises environment such as a data center. This can often reduce network costs, increase bandwidth throughput, and provide a stable network experience. Therefore, option 3 is the correct answer.

Other options are inappropriate as they are not high performance, leased line connectivity services.

Option 1 is incorrect. VPC peering is a function used to connect between two VPCs. It does not provide a connection function with an on-premises environment using a dedicated line.

Option 2 is incorrect. VPN is not a dedicated line connection, but a network connection using the Internet.

Option 4 is incorrect. The Internet gateway is a gateway used for communication between the VPC and the Internet.

Question 2:

The engineering team at an e-commerce company wants to establish a dedicated, encrypted, low latency, and high throughput connection between its data center and AWS Cloud. The engineering team has set aside sufficient time to account for the operational overhead of establishing this connection.

As a solutions architect, which of the following solutions would you recommend to the company?

Options:

- A. Use AWS Direct Connect plus VPN to establish a connection between the data center and AWS Cloud
- B. Use site-to-site VPN to establish a connection between the data center and AWS Cloud
- C. Use VPC transit gateway to establish a connection between the data center and AWS Cloud
- D. Use AWS Direct Connect to establish a connection between the data center and AWS Cloud

Answer: A

Explanation

Correct option:

Use AWS Direct Connect plus VPN to establish a connection between the data center and AWS Cloud

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations.

With AWS Direct Connect plus VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC VPN. This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.

This solution combines the AWS managed benefits of the VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection. Therefore, AWS Direct Connect plus VPN is the correct solution for this use-case.

Incorrect options:

Use site-to-site VPN to establish a connection between the data center and AWS Cloud – AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). A VPC VPN Connection utilizes IPsec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity. However, Site-to-site VPN cannot provide low latency and high throughput connection, therefore this option is ruled out.



Use VPC transit gateway to establish a connection between the data center and AWS Cloud – A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks. A transit gateway by itself cannot establish a low latency and high throughput connection between a data center and AWS Cloud. Hence this option is incorrect.

Use AWS Direct Connect to establish a connection between the data center and AWS Cloud – AWS Direct Connect by itself cannot provide an encrypted connection between a data center and AWS Cloud, so this option is ruled out.

74. Setting Up a VPN Over a Direct Connect Connection

75. Global Accelerator

Question 1:

A new application is to be published in multiple regions around the world. The Architect needs to ensure only 2 IP addresses need to be whitelisted. The solution should intelligently route traffic for lowest latency and provide fast regional failover.

How can this be achieved?

Options:

- A. Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator
- B. Launch EC2 instances into multiple regions behind an NLB with a static IP address
- C. Launch EC2 instances into multiple regions behind an ALB and use a Route 53 failover routing policy
- D. Launch EC2 instances into multiple regions behind an ALB and use Amazon CloudFront with a pair of static IP addresses

Answer: A

Explanation

AWS Global Accelerator uses the vast, congestion-free AWS global network to route TCP and UDP traffic to a healthy application endpoint in the closest AWS Region to the user.

This means it will intelligently route traffic to the closest point of presence (reducing latency). Seamless failover is ensured as AWS Global Accelerator uses anycast IP address which means the IP does not change when failing over between regions so there are no issues with client caches having incorrect entries that need to expire.

This is the only solution that provides deterministic failover.

CORRECT: “Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator” is the correct answer.

INCORRECT: “Launch EC2 instances into multiple regions behind an NLB with a static IP address” is incorrect. An NLB with a static IP is a workable solution as you could configure a primary and secondary address in applications. However, this solution does not intelligently route traffic for lowest latency.

INCORRECT: “Launch EC2 instances into multiple regions behind an ALB and use a Route 53 failover routing policy” is incorrect. A Route 53 failover routing policy uses a primary and standby configuration. Therefore, it sends all traffic to the primary until it fails a health check at which time it sends traffic to the secondary. This solution does not intelligently route traffic for lowest latency.

INCORRECT: “Launch EC2 instances into multiple regions behind an ALB and use Amazon CloudFront with a pair of static IP addresses” is incorrect. Amazon CloudFront cannot be configured with “a pair of static IP addresses”.

Question 2:

A gaming company is looking at improving the availability and performance of its global flagship application which utilizes UDP protocol and needs to support fast regional failover in case an AWS Region goes down.

Which of the following AWS services represents the best solution for this use-case?

Options:

- A. Amazon CloudFront
- B. AWS Elastic Load Balancing (ELB)
- C. Amazon Route 53
- D. AWS Global Accelerator

Answer: D

Explanation

Correct option:

AWS Global Accelerator – AWS Global Accelerator utilizes the Amazon global network, allowing you to improve the performance of your applications by lowering first-byte latency (the round trip time for a packet to go from a client to your endpoint and back again) and jitter (the variation of latency), and increasing throughput (the amount of time it takes to transfer data) as compared to the public internet.

Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

Incorrect options:

Amazon CloudFront – Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery), while Global Accelerator improves performance for a wide range of applications over TCP or UDP.

AWS Elastic Load Balancing (ELB) – Both of the services, ELB and Global Accelerator solve the challenge of routing user requests to healthy application endpoints. AWS Global Accelerator relies on ELB to provide the traditional load balancing features such as support for internal and non-AWS endpoints, pre-warming, and Layer 7 routing. However, while ELB provides load balancing within one Region, AWS Global Accelerator provides traffic management across multiple Regions.

A regional ELB load balancer is an ideal target for AWS Global Accelerator. By using a regional ELB load balancer, you can precisely distribute incoming application traffic across backends, such as Amazon EC2 instances or Amazon ECS tasks, within an AWS Region.

If you have workloads that cater to a global client base, AWS recommends that you use AWS Global Accelerator. If you have workloads hosted in a single AWS Region and used by clients in and around the same Region, you can use an Application Load Balancer or Network Load Balancer to manage your resources.

Amazon Route 53 – Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like `www.example.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect to each other.

76. VPC End Points

Question 1:

A company wishes to restrict access to their Amazon DynamoDB table to specific, private source IP addresses from their VPC. What should be done to secure access to the table?

Options:

- A. Create the Amazon DynamoDB table in the VPC
- B. Create a gateway VPC endpoint and add an entry to the route table
- C. Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)
- D. Create an AWS VPN connection to the Amazon DynamoDB endpoint

Answer: B

Explanation

There are two different types of VPC endpoint: interface endpoint, and gateway endpoint. With an interface endpoint you use an ENI in the VPC. With a gateway endpoint you configure your route table to point to the endpoint. Amazon S3 and DynamoDB use gateway endpoints. This solution means that all traffic will go through the VPC endpoint straight to DynamoDB using private IP addresses.

CORRECT: “Create a gateway VPC endpoint and add an entry to the route table” is the correct answer.

INCORRECT: “Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)” is incorrect. ↑ mentioned above, an interface endpoint is not used for DynamoDB, you must use a gateway endpoint.

INCORRECT: “Create the Amazon DynamoDB table in the VPC” is incorrect. You cannot create a DynamoDB table in a VPC, to connect securely using private addresses you should use a gateway endpoint instead.

INCORRECT: “Create an AWS VPN connection to the Amazon DynamoDB endpoint” is incorrect. You cannot create an AWS VPN connection to the Amazon DynamoDB endpoint.

77. VPC Private Link

78. Transit Gateway

Question 01:

A company has many VPC in various accounts, that need to be connected in a star network with one another and connected with on-premises networks through Direct Connect.

What do you recommend?

- VPC Peering
- VPN Gateway
- Transit Gateway (Correct)
- Private Link

Explanation

Correct option:

Transit Gateway

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. With AWS Transit Gateway, you only have to create and manage a single connection from the central gateway into each Amazon VPC, on-premises data center, or remote office across your network. Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. So, this is a perfect use-case for the Transit Gateway.

Incorrect options:

VPC Peering – A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection). VPC Peering helps connect two VPCs and is not transitive. It would require to create many peering connections between all the VPCs to have them connect. This alone wouldn't work, because we would need to also connect the on-premises data center through Direct Connect and Direct Connect Gateway, but that's not mentioned in this answer.

VPN Gateway – A virtual private gateway (also known as a VPN Gateway) is the endpoint on the VPC side of your VPN connection. You can create a virtual private gateway before creating the VPC itself. VPN Gateway is a distractor here because we haven't mentioned a VPN.

Private Link – AWS PrivateLink simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet. AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. Private Link is utilized to create a private connection between an application that is fronted by an NLB in an account, and an Elastic Network Interface (ENI) in another account, without the need of VPC peering, and allowing the connections between the two to remain within the AWS network.

79. VPN Hub

Question 1:

Your company has decided to move from an on-premises environment to AWS. It's Tuesday now, and the data migration should be completed in 72 hours, starting from Friday night and finishing by Monday morning. This is done so that the migration doesn't affect business operations. The data capacity for migration is 10TB, and it is necessary to protect the migration data through secure communication.

Select a migration method that meets this condition.

Options:

- A. Data migration with Snowball
- B. Data transfer via Direct Connect connection
- C. Data transfer via VPN connection using AWS site-to-site VPN
- D. Data transfer by Storage Gateway

Answer: C

Explanation

Option 3 is the correct answer. Instances launched in Amazon VPC cannot communicate with your on-premises network by default. Therefore, you need to connect your data center or office network to AWS through an AWS site-to-Site VPN (Site-to-Site VPN) connection. You can then use Internet Protocol Security (IPsec) communication to create an encrypted VPN tunnel between the two points.

In this scenario, you need to choose a migration method based on the amount of migration data and the migration schedule. It is difficult to order Direct Connect or Snowball from AWS and perform the migration on the weekend because it is Tuesday now and the data transfer is to be carried out on the weekend. This is important because these preparations require time to coordinate with AWS, more time than on offer in this scenario. The only means that can be implemented immediately is VPN connection settings. In addition, 10TB of data transfer can easily be completed in 72 hours by transfer via VPN connection.

Option 1 is incorrect. Snowball uses equipment borrowed from AWS. It is convenient when the amount of data is large, but it is not suitable for short-notice and for such a small amount of data.

Option 2 is incorrect. Direct Connect physically requires the AWS side to set up a dedicated line connection settings. This requires application and settings to AWS, and may not be ready in time.

Option 4 is incorrect. Storage Gateway is used for data transfer and backup configuration between S3 and on-premises storage. It can also be used for data migration of storage, but this time it is inappropriate because it is not only storage that we targeted for data migration in this scenario.

80. Networking Costs

81. ELB

Question 1:

You are building a two-tier web application that delivers content while processing transactions on AWS. The data layer utilizes an online transaction processing (OLTP) database. At the WEB layer, it is necessary to create a flexible and scalable architectural configuration.

Choose the best way to meet this requirement.

Options:

- A. Set up ELB and Auto Scaling groups on your EC2 instance
- B. Set up a multi-AZ configuration for RDS
- C. Deploy EC2 instances in multi-AZ to configure failover routing with Route53
- D. Launch more EC2 instances than expected capacity

Answer: A

Explanation

Option 1 is the correct answer. This can be achieved by configuring Auto Scaling and ELB on your EC2 instance for flexible and scalable server processing on AWS. ELB distributes traffic to multiple instances for increased redundancy, and Auto Scaling automatically scales under heavy load.

Option 2 is incorrect. Since it is a requirement to create a flexible and scalable architecture configuration in the WEB layer, the setting of the RDS multi-AZ configuration in the database layer is incorrect.

Option 3 is incorrect. Failover routing with Route53 does not meet your requirements. Failover routing improves fault tolerance, but not performance.

Option 4 is incorrect. Placing more EC2 instances than the expected capacity requirement is incorrect because it ↑ not meet the requirements for flexible configuration.

Question 2:

An e-commerce application is hosted in AWS. The last time a new product was launched, the application experienced a performance issue due to an enormous spike in traffic. Management decided that capacity must be doubled this week after the product is launched.

What is the MOST efficient way for management to ensure that capacity requirements are met?

Options:

- A. Add a Step Scaling Policy
- B. Add a Scheduled Scaling Action
- C. Add a Simple Scaling Policy
- D. Add Amazon EC2 Spot instances

Answer: B

Explanation

Scaling based on a schedule allows you to set your own scaling schedule for predictable load changes. To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. This is ideal for situations where you know when and for how long you are going to need the additional capacity.

CORRECT: “Add a Scheduled Scaling action” is the correct answer.

INCORRECT: “Add a Step Scaling policy” is incorrect. Step scaling policies increase or decrease the current capacity of your Auto Scaling group based on a set of scaling adjustments, known as step adjustments. The adjustments vary based on the size of the alarm breach. This is more suitable to situations where the load unpredictable.

INCORRECT: “Add a Simple Scaling policy” is incorrect. AWS recommend using step over simple scaling in most cases. With simple scaling, after a scaling activity is started, the policy must wait for the scaling activity or health check replacement to complete and the cooldown period to expire before responding to additional alarms (in contrast to step scaling). Again, this is more suitable to unpredictable workloads.

INCORRECT: “Add Amazon EC2 Spot instances” is incorrect. Adding spot instances may decrease EC2 costs but you still need to ensure they are available. The main requirement of the question is that the performance issues are resolved rather than the cost being minimized.

Question 3:

A solutions architect has created a new Application Load Balancer and has configured a target group with IP address as a target type.

Which of the following types of IP addresses are allowed as a valid value for this target type?

Options:

- A. Elastic IP address
- B. Public IP address
- C. Dynamic IP address
- D. Private IP address

Answer: D

Explanation

Correct option:

Private IP address

When you create a target group, you specify its target type, which can be an Instance, IP or a Lambda function.

For IP address target type, you can route traffic using any private IP address from one or more network interfaces.

Incorrect options:

Public IP address

Elastic IP address

You can't specify publicly routable IP addresses as values for IP target type, so both these options are incorrect.

Dynamic IP address - There is no such thing as a dynamic IP address. This option has been added as a distractor.

Question 30:

You would like to deploy an application behind an Application Load Balancer, that will have some Auto Scaling capability and efficiently leverage a mix of Spot Instances and On-Demand instances to meet demand.

What do you recommend to manage the instances?

- A• Create a Spot Instance Request
- B• Create an ASG with a launch template



- C• Create a Spot Fleet Request
- D• Create an ASG with a launch configuration

Answer: B

Explanation

Correct option:

Create an ASG with a launch template

A launch configuration is an instance configuration template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping.

A launch template is similar to a launch configuration, in that it specifies instance configuration information. Included are the ID of the Amazon Machine Image (AMI), the instance type, a key pair, security groups, and the other parameters that you use to launch EC2 instances. However, defining a launch template instead of a launch configuration allows you to have multiple versions of a template.

Launch Templates do support a mix of On-Demand and Spot instances, and thanks to the ASG, we get auto-scaling capabilities. Hence this is the correct option.

Incorrect options:

Create a Spot Instance Request – A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price.

Spot Instance Requests only help to launch spot instances so we have to rule that out.

Create a Spot Fleet Request – Spot Fleet requests will help launch a mix of On-Demand and Spot, but won't have the auto-scaling capability we need. So this option is incorrect.

Create an ASG with a launch configuration – ASG Launch Configurations do not support a mix of On-Demand and Spot instances. So this option is incorrect as well.

Question 34:

The development team at an e-commerce startup has set up multiple microservices running on EC2 instances under an Elastic Load Balancer. The team wants to route traffic to multiple back-end services based on the content of the request.

Which of the following types of load balancers would allow routing based on the content of the request?

- A• Classic Load Balancer
- B• Both Application Load Balancer and Network Load Balancer
- C• Application Load Balancer
- D• Network Load Balancer

Answer: C

Explanation

Correct option:

Application Load Balancer

An Application Load Balancer functions at the application layer, the seventh layer of the Open Systems Interconnection (OSI) model. After the load balancer receives a request, it evaluates the listener rules in priority order to determine which rule to apply and then selects a target from the target group for the rule action. You can configure listener rules to route requests to different target groups based on the content of the application traffic. Each target group can be an independent microservice, therefore this option is correct.

Incorrect options:

Network Load Balancer – Network Load Balancer operates at the connection level (Layer 4), routing connections to targets – Amazon EC2 instances, microservices, and containers – within Amazon Virtual Private Cloud (Amazon VPC) based on IP protocol data.

Classic Load Balancer – Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network.

Network Load Balancer or Classic Load Balancer cannot be used to route traffic based on the content of the request. So both these options are incorrect.

Both Application Load Balancer and Network Load Balancer – Network Load Balancer cannot be used to route traffic based on the content of the request. So this option is also incorrect.

82. ELBs and Health Checks – LAB**83. Advanced ELB**

84. ASG**Question 1:**

You have set up an Auto Scaling group to increase the availability of your infrastructure. However, due to a configuration issue, the group was unable to launch the instance for more than 30 hours, even if the Auto Scaling configuration criteria were met.

Given this situation, what would Auto scaling's action/reaction be?

Options:

- A. Auto Scaling will continue to try launching an instance for up to 48 hours
- B. Auto Scaling stops the startup process
- C. Auto Scaling begins the startup process in another AZ
- D. Auto Scaling notifies CloudWatch when it fails to start

Answer: B

Explanation

If Auto Scaling encounters a problem when launching an instance, Auto Scaling will suspend processes running within that group and this can be restarted later on at any time. You would use this time to analyze configuration issues. Therefore, option 2 is the correct answer.

Question 2:

A company runs an application on six web application servers in an Amazon EC2 Auto Scaling group in a single Availability Zone. The application is fronted by an Application Load Balancer (ALB). A Solutions Architect needs to modify the infrastructure to be highly available without making any modifications to the application.

Which architecture should the Solutions Architect choose to enable high availability?

Options:

- A. Create an Auto Scaling group to launch three instances across each of two Regions
- B. Modify the Auto Scaling group to use two instances across each of three Availability Zones
- C. Create an Amazon CloudFront distribution with a custom origin across multiple Regions
- D. Create a launch template that can be used to quickly create more instances in another Region

Answer: B

Explanation

The only thing that needs to be changed in this scenario to enable HA is to split the instances across multiple Availability Zones. The architecture already uses Auto Scaling and Elastic Load Balancing so there is plenty of resilience to failure. Once the instances are running across multiple AZs there will be AZ-level fault tolerance as well.

CORRECT: “Modify the Auto Scaling group to use two instances across each of three Availability Zones” is the correct answer.

INCORRECT: “Create an Amazon CloudFront distribution with a custom origin across multiple Regions” is incorrect. CloudFront is not used to create HA for your application, it is used to accelerate access to media content.

INCORRECT: “Create a launch template that can be used to quickly create more instances in another Region” is incorrect. Multi-AZ should be enabled rather than multi-Region.

INCORRECT: “Create an Auto Scaling group to launch three instances across each of two Regions” is incorrect. HA can be achieved within a Region by simply enabling more AZs in the ASG. An ASG cannot launch instances in multiple Regions.

Question 3:

A company hosts a multiplayer game on AWS. The application uses Amazon EC2 instances in a single Availability Zone and users connect over Layer 4. Solutions Architect has been tasked with making the architecture highly available and also more cost-effective.

How can the solutions architect best meet these requirements? (Select TWO.)

- A. Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically
- B. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically
- C. Configure a Network Load Balancer in front of the EC2 instances



D. Increase the number of instances and use smaller EC2 instance types

E. Configure an Application Load Balancer in front of the EC2 instances

Answer: B & C

Explanation

The solutions architect must enable high availability for the architecture and ensure it is cost-effective. To enable high availability an Amazon EC2 Auto Scaling group should be created to add and remove instances across multiple availability zones. In order to distribute the traffic to the instances the architecture should use a Network Load Balancer which operates at Layer 4. This architecture will also be cost-effective as the Auto Scaling group will ensure the right number of instances are running based on demand.

CORRECT: “Configure a Network Load Balancer in front of the EC2 instances” is a correct answer.

CORRECT: “Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically” is also a correct answer.

INCORRECT: “Increase the number of instances and use smaller EC2 instance types” is incorrect as this is not the most cost-effective option. Auto Scaling should be used to maintain the right number of active instances.

INCORRECT: “Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically” is incorrect as this is not highly available as it’s a single AZ.

INCORRECT: “Configure an Application Load Balancer in front of the EC2 instances” is incorrect as an ALB operates at Layer 7 rather than Layer 4.

Question 4:

The payroll department at a company initiates several computationally intensive workloads on EC2 instances at a designated hour on the last day of every month. The payroll department has noticed a trend of severe performance lag during this hour. The engineering team has figured out a solution by using Auto Scaling Group for these EC2 instances and making sure that 10 EC2 instances are available during this peak usage hour. For normal operations only 2 EC2 instances are enough to cater to the workload.

As a solutions architect, which of the following steps would you recommend to implement the solution?

Options:

A. Configure your Auto Scaling group by creating a scheduled action that kicks-off at the designated hour on the last day of the month. Set the desired capacity of instances to 10. This causes the scale-out to happen before peak traffic kicks in at the designated hour

B. Configure your Auto Scaling group by creating a scheduled action that kicks-off at the designated hour on the last day of the month. Set the min count as well as the max count of instances to 10. This causes the scale-out to happen before peak traffic kicks in at the designated hour

C. Configure your Auto Scaling group by creating a target tracking policy and setting the instance count to 10 at the designated hour. This causes the scale-out to happen before peak traffic kicks in at the designated hour

D. Configure your Auto Scaling group by creating a simple tracking policy and setting the instance count to 10 at the designated hour. This causes the scale-out to happen before peak traffic kicks in at the designated hour

Answer: A

Explanation

Correct option:

Configure your Auto Scaling group by creating a scheduled action that kicks-off at the designated hour on the last day of the month. Set the desired capacity of instances to 10. This causes the scale-out to happen before peak traffic kicks in at the designated hour

Scheduled scaling allows you to set your own scaling schedule. For example, let's say that every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling actions based on the predictable traffic patterns of your web application. Scaling actions are performed automatically as a function of time and date.

A scheduled action sets the minimum, maximum, and desired sizes to what is specified by the scheduled action at the time specified by the scheduled action. For the given use case, the correct solution is to set the desired capacity to 10. When we want to specify a range of instances, then we must use min and max values.

Incorrect options:

Configure your Auto Scaling group by creating a scheduled action that kicks-off at the designated hour on the 1st day of the month. Set the min count as well as the max count of instances to 10. This causes the scale-out to happen before peak traffic kicks in at the designated hour - As mentioned earlier in the explanation, only when we want to specify a range of instances, then

we must use min and max values. As the given use-case requires exactly 10 instances to be available during the peak hour, so we must set the desired capacity to 10. Hence this option is incorrect.

Configure your Auto Scaling group by creating a target tracking policy and setting the instance count to 10 at the designated hour. This causes the scale-out to happen before peak traffic kicks in at the designated hour

Configure your Auto Scaling group by creating a simple tracking policy and setting the instance count to 10 at the designated hour. This causes the scale-out to happen before peak traffic kicks in at the designated hour

Target tracking policy or simple tracking policy cannot be used to effect a scaling action at a certain designated hour. Both these options have been added as distractors.

Question 5:

A social gaming startup has its flagship application hosted on a fleet of EC2 servers running behind an Elastic Load Balancer. These servers are part of an Auto Scaling Group. 90% of the users start logging into the system at 6 pm every day and continue till midnight. The engineering team at the startup has observed that there is a significant performance lag during the initial hour from 6 pm to 7 pm. The application is able to function normally thereafter.

As a solutions architect, which of the following steps would you recommend addressing the performance bottleneck during that initial hour of traffic spike?

- A. Configure your Auto Scaling group by creating a scheduled action that kicks-off before 6 pm. This causes the scale-out to happen even before peak traffic kicks in at 6 pm
- B. Configure your Auto Scaling group by creating a lifecycle hook that kicks-off before 6 pm. This causes the scale-out to happen even before peak traffic kicks in at 6 pm
- C. Configure your Auto Scaling group by creating a target tracking policy. This causes the scale-out to happen even before peak traffic kicks in at 6 pm
- D. Configure your Auto Scaling group by creating a step scaling policy. This causes the scale-out to happen even before peak traffic kicks in at 6 pm

Answer: A

Explanation

Correct option:

Configure your Auto Scaling group by creating a scheduled action that kicks-off before 6 pm. This causes the scale-out to happen even before peak traffic kicks in at 6 pm

The scheduled action tells the Amazon EC2 Auto Scaling group to perform a scaling action at specified times. To create a scheduled scaling action, you specify the start time when the scaling action should take effect, and the new minimum, maximum, and desired sizes for the scaling action. For the given use-case, the engineering team can create a daily scheduled action to kick-off before 6 pm which would cause the scale-out to happen even before peak traffic kicks in at 6 pm. Hence this is the correct option.

Incorrect options:

Configure your Auto Scaling group by creating a lifecycle hook that kicks-off before 6 pm. This causes the scale-out to happen even before peak traffic kicks in at 6 pm - Auto Scaling group lifecycle hooks enable you to perform custom actions as the Auto Scaling group launches or terminates instances. For example, you could install or configure software on newly launched instances, or download log files from an instance before it terminates. Therefore, lifecycle hooks cannot cause a scale-out to happen at a specified time. Hence this option is incorrect.

Configure your Auto Scaling group by creating a target tracking policy. This causes the scale-out to happen even before peak traffic kicks in at 6 pm - With target tracking scaling policies, you choose a scaling metric and set a target value. Application Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. Target tracking policy cannot cause a scale-out to happen at a specified time. Hence this option is incorrect.

Configure your Auto Scaling group by creating a step scaling policy. This causes the scale-out to happen even before peak traffic kicks in at 6 pm - With step scaling, you choose scaling metrics and threshold values for the CloudWatch alarms that trigger the scaling process as well as define how your scalable target should be scaled when a threshold is breached for a specified number of evaluation periods. Step scaling policy cannot cause a scale-out to happen at a specified time. Hence this option is incorrect.

In addition, both the target tracking as well as step scaling policies entail a lag wherein the instances will be provisioned only when the underlying CloudWatch alarms go off. Therefore we would still see performance lag during some part of the initial hour.

Question 6:

The DevOps team at an e-commerce company wants to perform some maintenance work on a specific EC2 instance that is part of an Auto Scaling group using a step scaling policy. The team is facing a maintenance challenge – every time the team deploys a maintenance patch, the instance health check status shows as out of service for a few minutes. This causes the Auto Scaling group to provision another replacement instance immediately.

As a solutions architect, which are the MOST time/resource efficient steps that you would recommend so that the maintenance work can be completed at the earliest? (Select two)

Options:

- A. Take a snapshot of the instance, create a new AMI and then launch a new instance using this AMI. Apply the maintenance patch to this new instance and then add it back to the Auto Scaling Group by using the manual scaling policy. Terminate the earlier instance that had the maintenance issue
- B. Put the instance into the Standby state and then update the instance by applying the maintenance patch. Once the instance is ready, you can exit the Standby state and then return the instance to service
- C. Delete the Auto Scaling group and apply the maintenance fix to the given instance. Create a new Auto Scaling group and add all the instances again using the manual scaling policy
- D. Suspend the ReplaceUnhealthy process type for the Auto Scaling group and apply the maintenance patch to the instance. Once the instance is ready, you can manually set the instance's health status back to healthy and activate the ReplaceUnhealthy process type again
- E. Suspend the ScheduledActions process type for the Auto Scaling group and apply the maintenance patch to the instance. Once the instance is ready, you can manually set the instance's health status back to healthy and activate the ScheduledActions process type again

Answer: B & D

Explanation

Correct options:

Put the instance into the Standby state and then update the instance by applying the maintenance patch. Once the instance is ready, you can exit the Standby state and then return the instance to service – You can put an instance that is in the InService state into the Standby state, update some software or troubleshoot the instance, and then return the instance to service. Instances that are on standby are still part of the Auto Scaling group, but they do not actively handle application traffic.

Suspend the ReplaceUnhealthy process type for the Auto Scaling group and apply the maintenance patch to the instance. Once the instance is ready, you can manually set the instance's health status back to healthy and activate the ReplaceUnhealthy process type again – The ReplaceUnhealthy process terminates instances that are marked as unhealthy and then creates new instances to replace them. Amazon EC2 Auto Scaling stops replacing instances that are marked as unhealthy. Instances that fail EC2 or Elastic Load Balancing health checks are still marked as unhealthy. As soon as you resume the ReplaceUnhealthy process, Amazon EC2 Auto Scaling replaces instances that were marked unhealthy while this process was suspended.

Incorrect options:

Take a snapshot of the instance, create a new AMI and then launch a new instance using this AMI. Apply the maintenance patch to this new instance and then add it back to the Auto Scaling Group by using the manual scaling policy. Terminate the earlier instance that had the maintenance issue – Taking the snapshot of the existing instance to create a new AMI and then creating a new instance in order to apply the maintenance patch is not time/resource optimal, hence this option is ruled out.

Delete the Auto Scaling group and apply the maintenance fix to the given instance. Create a new Auto Scaling group and add all the instances again using the manual scaling policy – It's not recommended to delete the Auto Scaling group just to apply a maintenance patch on a specific instance.

Suspend the ScheduledActions process type for the Auto Scaling group and apply the maintenance patch to the instance. Once the instance is ready, you can manually set the instance's health status back to healthy and activate the ScheduledActions process type again – Amazon EC2 Auto Scaling does not execute scaling actions that are scheduled to run during the suspension period. This option is not relevant to the given use-case.

Question 07:

The engineering team at a data analytics company has observed that its flagship application functions at its peak performance when the underlying EC2 instances have a CPU utilization of about 50%. The application is built on a fleet of EC2 instances managed under an Auto Scaling group. The workflow requests are handled by an internal Application Load Balancer that routes the requests to the instances.

As a solutions architect, what would you recommend so that the application runs near its peak performance state?

Options:

- A. Configure the Auto Scaling group to use step scaling policy and set the CPU utilization as the target metric with a target value of 50%
- B. Configure the Auto Scaling group to use simple scaling policy and set the CPU utilization as the target metric with a target value of 50%
- C. Configure the Auto Scaling group to use target tracking policy and set the CPU utilization as the target metric with a target value of 50%
- D. Configure the Auto Scaling group to use a Cloudwatch alarm triggered on a CPU utilization threshold of 50%

Answer: C

Explanation

Correct option:

Configure the Auto Scaling group to use target tracking policy and set the CPU utilization as the target metric with a target value of 50%

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies.

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value.

For example, you can use target tracking scaling to:

Configure a target tracking scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 50 percent.

This meets the requirements specified in the given use-case and therefore, this is the correct option.

Incorrect options:

Configure the Auto Scaling group to use step scaling policy and set the CPU utilization as the target metric with a target value of 50%

Configure the Auto Scaling group to use simple scaling policy and set the CPU utilization as the target metric with a target value of 50%

With step scaling and simple scaling, you choose scaling metrics and threshold values for the CloudWatch alarms that trigger the scaling process. Neither step scaling nor simple scaling can be configured to use a target metric for CPU utilization, hence both these options are incorrect.

Configure the Auto Scaling group to use a Cloudwatch alarm triggered on a CPU utilization threshold of 50% - An Auto Scaling group cannot directly use a Cloudwatch alarm as the source for a scale-in or scale-out event, hence this option is incorrect.

Question 08:

A tax computation software runs on Amazon EC2 instances behind a Classic Load Balancer. The instances are managed by an Auto Scaling Group. The tax computation software has an optimization module, which can take up to 10 minutes to find the optimal answer.

How do you ensure that when the Auto Scaling Group initiates a scale-in event, the users do not see their current requests interrupted?

- Increase the deregistration delay to more than 10 minutes (Correct)
- Enable Stickiness on the CLB
- Enable ELB health checks on the ASG
- Create an ASG Scheduled Action

Explanation

Correct option:

Increase the deregistration delay to more than 10 minutes

Elastic Load Balancing stops sending requests to targets that are deregistering. By default, Elastic Load Balancing waits 300 seconds before completing the deregistration process, which can help in-flight requests to the target to complete. We need to update this value to more than 10 minutes to allow our tax software to complete in-flight requests. Therefore this is the correct option.

Incorrect options:

Create an ASG Scheduled Action - Scheduled scaling allows you to set your scaling schedule. For example, let's say that every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts ↑ increase on Friday. You can plan your scaling actions based on the predictable traffic patterns of your web application. Scaling actions are performed automatically as a function of time and date.

You cannot use a scheduled action to stop the current request from being interrupted in case of a scale-in event. Hence this option is incorrect.

Enable Stickiness on the CLB – By default, a Classic Load Balancer routes each request independently to the registered instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance. You cannot use sticky sessions to stop the current request from being interrupted in case of a scale-in event. Hence this option is incorrect.

Enable ELB health checks on the ASG – The default health checks for an Auto Scaling group are EC2 status checks only. If an instance fails these status checks, the Auto Scaling group considers the instance unhealthy and replaces it. To ensure that the group can determine an instance's health based on additional tests provided by the load balancer, you can optionally configure the Auto Scaling group to use Elastic Load Balancing health checks.

ELB health checks, when enabled on an ASG, help let the ASG know when instances are unhealthy and trigger a scale-in event. You cannot use ELB health checks on the ASG to stop the current request from being interrupted in case of a scale-in event. Hence this option is incorrect.

85. Launch Configurations & Autoscaling Groups Lab

86. HA Architecture

87. Building a fault tolerant WordPress site – Lab 1

88. Building a fault tolerant WordPress site – Lab 2

89. Building a fault tolerant WordPress site – Lab 3 : Adding Resilience & Autoscaling

90. Building a fault tolerant WordPress site – Lab 4 : Cleaning Up

91. Building a fault tolerant WordPress site – Lab 5 : Cloud Formation

92. Elastic Beanstalk Lab

93. Highly Available Bastions

94. On Premise Strategies

95. SQS

Question 1:

Your company operates an application for uploading, processing and publishing user-submitted videos. This application is hosted on an EC2 instance for processing videos uploaded by users. It has an EC2 worker process that processes and publishes the video and also has an Auto Scaling group set up.

Select the services you should use to increase the reliability of your worker processes.

Options:

- A. SQS
- B. SNS
- C. SES
- D. CloudFront

Answer: A

Explanation:

Amazon SQS is used for decentralization, like with worker processing. The video processing request of the worker process is stored in the queue, enabling reliable processing execution by asynchronous processing. Multiple “worker” processes can be executed in parallel by distributing EC2 instances for use, responding to requests in the queue. Each message is consumed only once.

Distributed parallel processing of SQS queues can increase the reliability of worker processes. Therefore, option A is the correct answer.

Option 2 is incorrect. Messaging is the primary role of Amazon SNS and is used to configure worker processes to be triggered by specific events. SQS must be used to enable distributed processing of worker processes by queuing.

Option 3 is incorrect. You can implement the email function by using Amazon SES. SQS is used for distributed processing of worker processes.

Option 4 is incorrect. CloudFront is a service used for content distribution.

Question 2:

As a Solutions Architect, you are trying to add messaging processing using AWS messaging services to the application you are currently building. The most important requirement is to maintain the order of the messages and not send duplicate messages.

Which of the following services will help you meet this requirement?

Options:

- A. SQS
- B. SNS
- C. SES
- D. Lambda

Answer: A

Explanation

Option 1 is the correct answer. SQS is a managed message queuing service that allows you to monitor messages transferred between application components as queues. Utilizing FIFO queues enables high throughput, best effort ordering, and at least one delivery. FIFO queues guarantee message order and supports at least one message delivery.

Duplicate messages can be prevented by using the message deduplication ID in the SQS FIFO queue. The message deduplication ID is the token used to deduplicate the sent message. If a message with a specific message deduplication ID is sent successfully, the outgoing message with the same ID will not be delivered during the 5-minute deduplication interval.

Option 2 is incorrect. SNS is a push-type messaging service. The order of the messages sent is not guaranteed.

Option 3 is incorrect. SES is a service that can implement the email function. The order of the messages is not guaranteed as it only performs email notifications.

Option 4 is incorrect. Lambda does not have a message notification feature.

Question 3:

As a Solutions Architect, you are building a web application on AWS. This application provides data conversion services to users. The files to be converted are first uploaded to S3, and then a Spotfleet processes the data conversion. Users are divided into free users and paid users. Files submitted by paid users should be prioritized for processing.

Choose an solution that meets these requirements.

Options:

- A. Use Route53 to configure traffic routing according to customer type
- B. Use SQS to set a specific queue that preferentially processes paid users, and then use a regular queue for free users
- C. Use the Lambda function to send a message that allows preferentially processes of the paid users, and set the other as the default setting
- D. Use SNS to send the message that processing of paid users is to be processed preferentially, and set the other as the default setting

Answer: B

Explanation

SQS allows you to set priorities for queues. By doing so, it is possible to divide the queue further into queues that are processed preferentially and queues that are not. When each queue is polled separately, the higher priority queue is polled first. With this SQS setting, it is possible to set a queue to be processed preferentially for paid users and to use the default queue for free users. Therefore, option 2 is the correct answer.

Follow the settings for prioritization:

1. Prepare multiple queues for each priority using SQS.
2. Requests that are prioritized are to be placed in a high-priority queue.
3. Prepare the number of servers that process the queue based on their priority.
4. It is also possible to delay the processing start time by using the “delayed message transmission” function of the queue.

Question 4:

Your company has a database system that uses DynamoDB. Recently, due to the increase in the number of write processes, many processing delays and failures have occurred in the database. As a Solutions Architect, you are required to take action to ensure that write operations are not lost under any circumstances.

Choose the best way to meet this requirement.

Options:

- A. Use IOPS volume for DynamoDB
- B. Set up a distributed processing using SQS queues for DynamoDB write processing

C. Set up a distributed processing using SQS queue and set the Lambda function for the write process of DynamoDB

D. Perform DynamoDB data processing with an EC2 instance

Answer: C

Explanation

A “pending write request to the database” can be stored in the SQS queue for asynchronous processing. For DynamoDB data processing execution, it is also possible to execute DB processing by queue in cooperation with Lambda. By queuing the processing process, you can set the write processing queue so that it is not lost. This ensures that the request message is not lost, which meets the requirements. Therefore, option 3 is the correct answer.

Option 1 is incorrect. An IOPS volume configuration cannot be chosen for DynamoDB.

Option 2 is incorrect. The distributed processing process cannot be executed only with the SQS queue for the writing processing of DynamoDB. An SQS-triggered Lambda function is essential.

Option 4 is incorrect. Performing DynamoDB data processing with an EC2 instance is inefficient. DynamoDB data process can create more efficient architecture configurations by linking with Lambda function for serverless processing.

Question 5:

As a Solutions Architect, you are developing a workflow to send video data from your system to AWS for transcoding video data. We plan to build this mechanism using an EC2 worker instance that pulls transcode jobs from SQS.

Choose the correct feature of SQS that helps you complete this.

Options:

- A. SQS provides a health checks for worker instances
- B. SQS can achieve horizontal scaling
- C. SQS is best suited for this type of process because maintains the order of operations
- D. Processing according to a set schedule can be executed by SQS

Answer: B

Explanation

Option 2 is the correct answer. SQS allows load distribution by distributing system processing through queues. This helps you scale your AWS resources horizontally. SQS queues enable parallel processing with multiple EC2 instances, achieving load distribution and processing process optimization.

Option 1 is incorrect. SQS does not health check the status of worker instances.

Option 3 is incorrect. The order of the queues is not particularly important in this video processing, so it is not included as a requirement.

Option 4 is incorrect. SQS does not perform scheduled queuing.

Question 6:

A new application will run across multiple Amazon ECS tasks. Front-end application logic will process data and then pass that data to a back-end ECS task to perform further processing and write the data to a datastore. The Architect would like to reduce interdependencies so failures do no impact other components.

Which solution should the Architect use?

Options:

- A. Create an Amazon Kinesis Firehose delivery stream that delivers data to an Amazon S3 bucket, configure the front-end to write data to the stream and the back-end to read data from Amazon S3
- B. Create an Amazon Kinesis Firehose delivery stream and configure the front-end to add data to the stream and the back-end to read data from the stream
- C. Create an Amazon SQS queue that pushes messages to the back-end. Configure the front-end to add messages to the queue
- D. Create an Amazon SQS queue and configure the front-end to add messages to the queue and the back-end to poll the queue for messages

Answer: D

Explanation

This is a good use case for Amazon SQS. SQS is a service that is used for decoupling applications, thus reducing interdependencies, through a message bus. The front-end application can place messages on the queue and the back-end can then poll the queue for new messages. Please remember that Amazon SQS is pull-based (polling) not push-based (use SNS for push-based).

CORRECT: “Create an Amazon SQS queue and configure the front-end to add messages to the queue and the back-end to poll the queue for messages” is the correct answer.

INCORRECT: “Create an Amazon Kinesis Firehose delivery stream and configure the front-end to add data to the stream and the back-end to read data from the stream” is incorrect. Amazon Kinesis Firehose is used for streaming data. With Firehose the data is immediately loaded into a destination that can be Amazon S3, RedShift, Elasticsearch, or Splunk. This is not an ideal use case for Firehose as this is not streaming data and there is no need to load data into an additional AWS service.

INCORRECT: “Create an Amazon Kinesis Firehose delivery stream that delivers data to an Amazon S3 bucket, configure the front-end to write data to the stream and the back-end to read data from Amazon S3” is incorrect as per the previous explanation.

INCORRECT: “Create an Amazon SQS queue that pushes messages to the back-end. Configure the front-end to add messages to the queue ” is incorrect as SQS is pull-based, not push-based. EC2 instances must poll the queue to find jobs to process.

Question 7:

An eCommerce application consists of three tiers. The web tier includes EC2 instances behind an Application Load balancer, the middle tier uses EC2 instances and an Amazon SQS queue to process orders, and the database tier consists of an Auto Scaling DynamoDB table. During busy periods customers have complained about delays in the processing of orders. A Solutions Architect has been tasked with reducing processing times.

Which action will be MOST effective in accomplishing this requirement?

Options:

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

Answer: D

Explanation

The most likely cause of the processing delays is insufficient instances in the middle tier where the order processing takes place. The most effective solution to reduce processing times in this case is to scale based on the backlog per instance (number of messages in the SQS queue) as this reflects the amount of work that needs to be done.

CORRECT: “Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth” is the correct answer.

INCORRECT: “Replace the Amazon SQS queue with Amazon Kinesis Data Firehose” is incorrect. The issue is not the efficiency of queuing messages but the processing of the messages. In this case scaling the EC2 instances to reflect the workload is a better solution.

INCORRECT: “Use Amazon DynamoDB Accelerator (DAX) in front of the DynamoDB backend tier” is incorrect. The DynamoDB table is configured with Auto Scaling so this is not likely to be the bottleneck in order processing.

INCORRECT: “Add an Amazon CloudFront distribution with a custom origin to cache the responses for the web tier” is incorrect. This will cache media files to speed up web response times but not order processing times as they take place in the middle tier.

Question 8:

A web application allows users to upload photos and add graphical elements to them. The application offers two tiers of service: free and paid. Photos uploaded by paid users should be processed before those submitted using the free tier. The photos are uploaded to an Amazon S3 bucket which uses an event notification to send the job information to Amazon SQS.

How should a Solutions Architect configure the Amazon SQS deployment to meet these requirements?

Options:

- A. Use one SQS standard queue. Use batching for the paid photos and short polling for the free photos
- B. Use a separate SQS FIFO queue for each tier. Set the free queue to use short polling and the paid queue to use long polling
- C. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first
- D. Use a separate SQS Standard queue for each tier. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue

Answer: D

Explanation

AWS recommend using separate queues when you need to provide prioritization of work. The logic can then be implemented at the application layer to prioritize the queue for the paid photos over the queue for the free photos.

CORRECT: “Use a separate SQS Standard queue for each tier. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue” is the correct answer.

INCORRECT: “Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first” is incorrect. FIFO queues preserve the order of messages but they do not prioritize messages within the queue. The orders would need to be placed

into the queue in a priority order and there's no way of doing this as the messages are sent automatically through event notifications as they are received by Amazon S3.

INCORRECT: “Use one SQS standard queue. Use batching for the paid photos and short polling for the free photos” is incorrect. Batching adds efficiency but it has nothing to do with ordering or priority.

INCORRECT: “Use a separate SQS FIFO queue for each tier. Set the free queue to use short polling and the paid queue to use long polling” is incorrect. Short polling and long polling are used to control the amount of time the consumer process waits before closing the API call and trying again. Polling should be configured for efficiency of API calls and processing of messages but does not help with message prioritization.

Question 9:

A company is working with a strategic partner that has an application that must be able to send messages to one of the company's Amazon SQS queues. The partner company has its own AWS account.

How can a Solutions Architect provide least privilege access to the partner?

Options:

- A. Create a user account that and grant the sqs:SendMessage permission for Amazon SQS. Share the credentials with the partner company
- B. Update the permission policy on the SQS queue to grant all permissions to the partner's AWS account
- C. Update the permission policy on the SQS queue to grant the sqs:SendMessage permission to the partner's AWS account
- D. Create a cross-account role with access to all SQS queues and use the partner's AWS account in the trust document for the role

Answer: C

Explanation

Amazon SQS supports resource-based policies. The best way to grant the permissions using the principle of least privilege is to use a resource-based policy attached to the SQS queue that grants the partner company's AWS account the sqs:SendMessage privilege.

CORRECT: “Update the permission policy on the SQS queue to grant the sqs:SendMessage permission to the partner's AWS account” is the correct answer.

INCORRECT: “Create a user account that and grant the sqs:SendMessage permission for Amazon SQS. Share the credentials with the partner company” is incorrect. This would provide the permissions for all SQS queues, not just the queue the partner company should be able to access.

INCORRECT: “Create a cross-account role with access to all SQS queues and use the partner's AWS account in the trust document for the role” is incorrect. This would provide access to all SQS queues and the partner company should only be able to access one SQS queue.

INCORRECT: “Update the permission policy on the SQS queue to grant all permissions to the partner's AWS account” is incorrect. This provides too many permissions; the partner company only needs to send messages to the queue.

Question 10:

An application running on Amazon EC2 needs to asynchronously invoke an AWS Lambda function to perform data processing. The services should be decoupled.

Which service can be used to decouple the compute services?

Options:

- A. Amazon SNS
- B. AWS Step Functions
- C. Amazon MQ
- D. AWS Config

Answer: A

Explanation

You can use a Lambda function to process Amazon Simple Notification Service notifications. Amazon SNS supports Lambda functions as a target for messages sent to a topic. This solution decouples the Amazon EC2 application from Lambda and ensures the Lambda function is invoked.

CORRECT: “Amazon SNS” is the correct answer.

INCORRECT: “AWS Config” is incorrect. AWS Config is a service that is used for continuous compliance, not application decoupling.

INCORRECT: “Amazon MQ” is incorrect. Amazon MQ is similar to SQS but is used for existing applications that are being

migrated into AWS. SQS should be used for new applications being created in the cloud.

INCORRECT: “AWS Step Functions” is incorrect. AWS Step Functions is a workflow service. It is not the best solution for this scenario.

Question 11:

A major bank is using SQS to migrate several core banking applications to the cloud to ensure high availability and cost efficiency while simplifying administrative complexity and overhead. The development team at the bank expects a peak rate of about 1000 messages per second to be processed via SQS. It is important that the messages are processed in order.

Which of the following options can be used to implement this system?

Options:

- A. Use Amazon SQS FIFO queue in batch mode of 4 messages per operation to process the messages at the peak rate
- B. Use Amazon SQS FIFO queue to process the messages
- C. Use Amazon SQS standard queue to process the messages
- D. Use Amazon SQS FIFO queue in batch mode of 2 messages per operation to process the messages at the peak rate

Answer: A

Explanation

Correct option:

Use Amazon SQS FIFO queue in batch mode of 4 messages per operation to process the messages at the peak rate

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS offers two types of message queues – Standard queues vs FIFO queues.

For FIFO queues, the order in which messages are sent and received is strictly preserved (i.e. First-In-First-Out). On the other hand, the standard SQS queues offer best-effort ordering. This means that occasionally, messages might be delivered in an order different from which they were sent.

By default, FIFO queues support up to 300 messages per second (300 send, receive, or delete operations per second). When you batch 10 messages per operation (maximum), FIFO queues can support up to 3,000 messages per second. Therefore you need to process 4 messages per operation so that the FIFO queue can support up to 1200 messages per second, which is well within the peak rate.

Incorrect options:

Use Amazon SQS standard queue to process the messages – As messages need to be processed in order, therefore standard queues are ruled out.

Use Amazon SQS FIFO queue to process the messages – By default, FIFO queues support up to 300 messages per second and this is not sufficient to meet the message processing throughput per the given use-case. Hence this option is incorrect.

Use Amazon SQS FIFO queue in batch mode of 2 messages per operation to process the messages at the peak rate – As mentioned earlier in the explanation, you need to use FIFO queues in batch mode and process 4 messages per operation, so that the FIFO queue can support up to 1200 messages per second. With 2 messages per operation, you can only support up to 600 messages per second.

Question 5:

You are establishing a monitoring solution for desktop systems, that will be sending telemetry data into AWS every 1 minute. Data for each system must be processed in order, independently, and you would like to scale the number of consumers to be possibly equal to the number of desktop systems that are being monitored.

What do you recommend?

- Use an SQS FIFO queue, and make sure the telemetry data is sent with a Group ID attribute representing the value of the Desktop ID (Correct)
- Use an SQS FIFO queue, and send the telemetry data as is
- Use a Kinesis Data Stream, and send the telemetry data with a Partition ID that uses the value of the Desktop ID
- Use an SQS standard queue, and send the telemetry data as is

Explanation

Correct option:

Use an SQS FIFO queue, and make sure the telemetry data is sent with a Group ID attribute representing the value of the Desktop ID

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS offers two types of message queues. Standard queues offer

maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

We, therefore, need to use an SQS FIFO queue. If we don't specify a GroupID, then all the messages are in absolute order, but we can only have 1 consumer at most. To allow for multiple consumers to read data for each Desktop application, and to scale the number of consumers, we should use the "Group ID" attribute. So this is the correct option.

Incorrect options:

Use an SQS FIFO queue, and send the telemetry data as is – This is incorrect because if we send the telemetry data as is then we will not be able to scale the number of consumers to be equal to the number of desktop systems. In this case, each message will have its consumer. So we should use the "Group ID" attribute so that multiple consumers can read data for each Desktop application.

Use an SQS standard queue, and send the telemetry data as is – An SQS standard queue has no ordering capability so that's ruled out.

Use a Kinesis Data Stream, and send the telemetry data with a Partition ID that uses the value of the Desktop ID – Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. A Kinesis Data Stream would work and would give us the data for each desktop application within shards, but we can only have as many consumers as shards in Kinesis (which is in practice, much less than the number of producers).

96. SWF

97. SNS

Question 1:

The engineering team at a Spanish professional football club has built a notification system for its website using Amazon SNS notifications which are then handled by a Lambda function for end-user delivery. During the off-season, the notification systems need to handle about 100 requests per second. During the peak football season, the rate touches about 5000 requests per second and it is noticed that a significant number of the notifications are not being delivered to the end-users on the website.

As a solutions architect, which of the following would you suggest as the BEST possible solution to this issue?

Options:

- A. Amazon SNS message deliveries to AWS Lambda have crossed the account concurrency quota for Lambda, so the team needs to contact AWS support to raise the account limit
- B. Amazon SNS has hit a scalability limit, so the team needs to contact AWS support to raise the account limit
- C. The engineering team needs to provision more servers running the Lambda service
- D. The engineering team needs to provision more servers running the SNS service

Answer: A

Explanation

Correct option:

Amazon SNS message deliveries to AWS Lambda have crossed the account concurrency quota for Lambda, so the team needs to contact AWS support to raise the account limit

Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

With AWS Lambda, you can run code without provisioning or managing servers. You pay only for the compute time that you consume—there's no charge when your code isn't running.

AWS Lambda currently supports 1000 concurrent executions per AWS account per region. If your Amazon SNS message deliveries to AWS Lambda contribute to crossing these concurrency quotas, your Amazon SNS message deliveries will be throttled. You need to contact AWS support to raise the account limit. Therefore this option is correct.

Incorrect options:

Amazon SNS has hit a scalability limit, so the team needs to contact AWS support to raise the account limit ↑ azon SNS leverages the proven AWS cloud to dynamically scale with your application. You don't need to contact AWS support, as SNS is a fully managed service, taking care of the heavy lifting related to capacity planning, provisioning, monitoring, and patching.

Therefore, this option is incorrect.

The engineering team needs to provision more servers running the SNS service

The engineering team needs to provision more servers running the Lambda service

As both Lambda and SNS are serverless and fully managed services, the engineering team cannot provision more servers. Both of these options are incorrect.

Question 20: Skipped

A cybersecurity company uses a fleet of EC2 instances to run a proprietary application. The infrastructure maintenance group at the company wants to be notified via an email whenever the CPU utilization for any of the EC2 instances breaches a certain threshold.

Which of the following services would you use for building a solution with the LEAST amount of development effort? (Select two)

- Amazon SNS (Correct)
- AWS Lambda
- Amazon SQS
- Amazon CloudWatch (Correct)
- AWS Step Functions

Explanation

Correct options:

Amazon SNS – Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging.

Amazon CloudWatch – Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Amazon CloudWatch allows you to monitor AWS cloud resources and the applications you run on AWS.

You can use CloudWatch Alarms to send an email via SNS whenever any of the EC2 instances breaches a certain threshold. Hence both these options are correct.

Incorrect options:

AWS Lambda – With AWS Lambda, you can run code without provisioning or managing servers. You pay only for the compute time that you consume—there's no charge when your code isn't running. You can run code for virtually any type of application or backend service—all with zero administration. You cannot use AWS Lambda to monitor CPU utilization of EC2 instances or send notification emails, hence this option is incorrect.

Amazon SQS – Amazon SQS Standard offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows. You cannot use SQS to monitor CPU utilization of EC2 instances or send notification emails, hence this option is incorrect.

AWS Step Functions – AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. Using Step Functions, you can design and run workflows that stitch together services, such as AWS Lambda, AWS Fargate, and Amazon SageMaker, into feature-rich applications. You cannot use Step Functions to monitor CPU utilization of EC2 instances or send notification emails, hence this option is incorrect.

98. Elastic Transcoder

99. API Gateway

Question 1:

As a Solutions Architect, you are building business applications on a serverless architecture. In this application, the process of acquiring, registering, and changing DynamoDB data is performed by a Lambda function. You need to be able to call this application over HTTP.

How can this requirement be achieved?

Options:

- A. Install API Gateway and integrate with Lambda functions
- B. Set the IAM role to a Lambda function to allow HTTP access
- C. Set HTTP permissions in the Lambda function settings
- D. Configure NACLs to allow HTTP access to Lambda function

Answer: A

Explanation

Option 1 is the correct answer. The API gateway provides HTTP access to back-end services via the API. API gateway is a service that can be integrated with Lambda, and by implementing this setting to integrate API gateway with Lambda function, you can access Lambda function with HTTP.

Option 2 is incorrect. The IAM role allows one AWS resources to access another AWS resource. It is not a function that allows HTTP access.

Option 3 is incorrect. There is no function to allow HTTP access in the Lambda function settings.

Option 4 is incorrect. There is no ability to configure the network ACLs to allow HTTP access to Lambda functions.

Question 2:

The product team at a startup has figured out a market need to support both stateful and stateless client-server communications via the APIs developed using its platform. You have been hired by the startup as a solutions architect to build a solution to fulfill this market need using AWS API Gateway.

Which of the following would you identify as correct?

Options:

- A. API Gateway creates RESTful APIs that enable stateful client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server
- B. API Gateway creates RESTful APIs that enable stateless client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateless, full-duplex communication between client and server
- C. API Gateway creates RESTful APIs that enable stateful client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateless, full-duplex communication between client and server
- D. API Gateway creates RESTful APIs that enable stateless client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server

Answer: D

Explanation

Correct option:

API Gateway creates RESTful APIs that enable stateless client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the front door for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications.

API Gateway creates RESTful APIs that:

Are HTTP-based.

Enable stateless client-server communication.

Implement standard HTTP methods such as GET, POST, PUT, PATCH, and DELETE.

API Gateway creates WebSocket APIs that:

Adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server. Route incoming messages based on message content.

So API Gateway supports stateless RESTful APIs as well as stateful WebSocket APIs. Therefore this option is correct.

Incorrect options:

API Gateway creates RESTful APIs that enable stateful client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server

API Gateway creates RESTful APIs that enable stateless client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateless, full-duplex communication between client and server

API Gateway creates RESTful APIs that enable stateful client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateless, full-duplex communication between client and server

APIs that adhere to the WebSocket protocol, which enables stateless, full-duplex communication between client and server. These three options contradict the earlier details provided in the explanation. To summarize, API Gateway supports stateless RESTful APIs and stateful WebSocket APIs. Hence these options are incorrect.

Question 3:

A Big Data analytics company wants to set up an AWS cloud architecture that throttles requests in case of sudden traffic spikes. The company is looking for AWS services that can be used for buffering or throttling to handle such traffic variations. Which of the following services can be used to support this requirement?

Options:

- A. Amazon Gateway Endpoints, Amazon SQS and Amazon Kinesis
- B. Amazon API Gateway, Amazon SQS and Amazon Kinesis
- C. Elastic Load Balancer, Amazon SQS, AWS Lambda
- D. Amazon SQS, Amazon SNS and AWS Lambda

Answer: B

Explanation

Correct option:

Throttling is the process of limiting the number of requests an authorized program can submit to a given operation in a given amount of time.

Amazon API Gateway, Amazon SQS and Amazon Kinesis – To prevent your API from being overwhelmed by too many requests, Amazon API Gateway throttles requests to your API using the token bucket algorithm, where a token counts for a request. Specifically, API Gateway sets a limit on a steady-state rate and a burst of request submissions against all APIs in your account. In the token bucket algorithm, the burst is the maximum bucket size.

Amazon SQS – Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS offers buffer capabilities to smooth out temporary volume spikes without losing messages or increasing latency.

Amazon Kinesis – Amazon Kinesis is a fully managed, scalable service that can ingest, buffer, and process streaming data in real-time.

Incorrect options:

Amazon SQS, Amazon SNS and AWS Lambda – Amazon SQS has the ability to buffer its messages. Amazon Simple Notification Service (SNS) cannot buffer messages and is generally used with SQS to provide the buffering facility. AWS Lambda is a compute service and does not provide any buffering capability. So, this combination of services is incorrect.

Amazon Gateway Endpoints, Amazon SQS and Amazon Kinesis – A Gateway Endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. This cannot help in throttling or buffering of requests. Amazon SQS and Kinesis can buffer incoming data. Since Gateway Endpoint is an incorrect service for throttling or buffering, this option is incorrect.

Elastic Load Balancer, Amazon SQS, AWS Lambda – Elastic Load Balancer cannot throttle requests. Amazon SQS can be used to buffer messages. AWS Lambda cannot be used for buffering. So, this combination is also incorrect.

100. Kinesis

Question 1:

A company provides a REST-based interface to an application that allows a partner company to send data in near-real time. The application then processes the data that is received and stores it for later analysis. The application runs on Amazon EC2 instances.

The partner company has received many 503 Service Unavailable Errors when sending data to the application and the compute capacity reaches its limits and is unable to process requests when spikes in data volume occur.

Which design should a Solutions Architect implement to improve scalability?

Options:

- A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions
- B. Use Amazon API Gateway in front of the existing application. Create a usage plan with a quota limit for the partner company
- C. Use Amazon SNS to ingest the data and trigger AWS Lambda functions to process the data in near-real time
- D. Use Amazon SQS to ingest the data. Configure the EC2 instances to process messages from the SQS queue

Answer: A

Explanation

Amazon Kinesis enables you to ingest, buffer, and process streaming data in real-time. Kinesis can handle any amount of streaming data and process data from hundreds of thousands of sources with very low latencies. This is an ideal solution for data ingestion.

To ensure the compute layer can scale to process increasing workloads, the EC2 instances should be replaced by AWS Lambda functions. Lambda can scale seamlessly by running multiple executions in parallel.

CORRECT: “Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions” is the correct answer.

INCORRECT: “Use Amazon API Gateway in front of the existing application. Create a usage plan with a quota limit for the partner company” is incorrect. A usage plan will limit the amount of data that is received and cause more errors to be received by the partner company.

INCORRECT: “Use Amazon SQS to ingest the data. Configure the EC2 instances to process messages from the SQS queue” is incorrect. Amazon Kinesis Data Streams should be used for near-real time or real-time use cases instead of Amazon SQS.

INCORRECT: “Use Amazon SNS to ingest the data and trigger AWS Lambda functions to process the data in near-real time” is incorrect. SNS is not a near-real time solution for data ingestion. SNS is used for sending notifications.

Question 2:

A manufacturing company captures data from machines running at customer sites. Currently, thousands of machines send data every 5 minutes, and this is expected to grow to hundreds of thousands of machines in the near future. The data is logged with the intent to be analyzed in the future as needed.

What is the SIMPLEST method to store this streaming data at scale?

Options:

- A. Create an Amazon SQS queue, and have the machines write to the queue
- B. Create an Amazon EC2 instance farm behind an ELB to store the data in Amazon EBS Cold HDD volumes
- C. Create an Auto Scaling Group of Amazon EC2 instances behind ELBs to write data into Amazon RDS
- D. Create an Amazon Kinesis Firehose delivery stream to store the data in Amazon S3

Answer: D

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 you can deliver the data to “destinations” including Amazon S3 buckets for later analysis

CORRECT: “Create an Amazon Kinesis Firehose delivery stream to store the data in Amazon S3” is the correct answer.

INCORRECT: “Create an Amazon EC2 instance farm behind an ELB to store the data in Amazon EBS Cold HDD volumes” is incorrect. Storing the data in EBS would be expensive and as EBS volumes cannot be shared by multiple instances you would have a bottleneck of a single EC2 instance writing the data.

INCORRECT: “Create an Amazon SQS queue, and have the machines write to the queue” is incorrect. Using an SQS queue to store the data is not possible as the data needs to be stored long-term and SQS queues have a maximum retention time of 14 days.

INCORRECT: “Create an Auto Scaling Group of Amazon EC2 instances behind ELBs to write data into Amazon RDS” is incorrect. Writing data into RDS via a series of EC2 instances and a load balancer is more complex and more expensive. RDS is also not an ideal data store for this data.

Question 3:

A retail company with many stores and warehouses is implementing IoT sensors to gather monitoring data from devices in each location. The data will be sent to AWS in real time. A solutions architect must provide a solution for ensuring events are received in order for each device and ensure that data is saved for future processing.

Which solution would be MOST efficient?

Options:

- A. Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS
- D. Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose

to save data to Amazon S3

Answer: D

Explanation

Amazon Kinesis Data Streams collect and process data in real time. A Kinesis data stream is a set of shards. Each shard has a sequence of data records. Each data record has a sequence number that is assigned by Kinesis Data Streams. A shard is a uniquely identified sequence of data records in a stream.

A partition key is used to group data by shard within a stream. Kinesis Data Streams segregates the data records belonging to a stream into multiple shards. It uses the partition key that is associated with each data record to determine which shard a given data record belongs to.

CORRECT: “Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3” is the correct answer.

INCORRECT: “Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS” is incorrect as you cannot save data to EBS from Kinesis.

INCORRECT: “Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS” is incorrect as SQS is not the most efficient service for streaming, real time data.

INCORRECT: “Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3” is incorrect as SQS is not the most efficient service for streaming, real time data.

Question 4:

A geological research agency maintains the seismological data for the last 100 years. The data has a velocity of 1GB per minute. You would like to store the data with only the most relevant attributes to build a predictive model for earthquakes.

What AWS services would you use to build the most cost-effective solution with the LEAST amount of infrastructure maintenance?

Options:

- A. Ingest the data in a Spark Streaming Cluster on EMR use Spark Streaming transformations before writing to S3
- B. Ingest the data in AWS Glue job and use Spark transformations before writing to S3
- C. Ingest the data in Kinesis Data Firehose and use a Lambda function to filter and transform the incoming stream before the output is dumped on S3
- D. Ingest the data in Kinesis Data Analytics and use SQL queries to filter and transform the data before writing to S3

Answer: C

Explanation

Correct option:

Ingest the data in Kinesis Data Firehose and use a Lambda function to filter and transform the incoming stream before the output is dumped on S3

Amazon Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you’re already using today. It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. It can also batch, compress, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security.

The correct choice is to ingest the data in Kinesis Data Firehose and use a Lambda function to filter and transform the incoming data before the output is dumped on S3. This way you only store a sliced version of the data with only the relevant data attributes required for your model. Also it should be noted that this solution is entirely serverless and requires no infrastructure maintenance.

Incorrect options:

Ingest the data in Kinesis Data Analytics and use SQL queries to filter and transform the data before writing to S3 – Amazon Kinesis Data Analytics is the easiest way to analyze streaming data in real-time. Kinesis Data Analytics enables you to easily and quickly build queries and sophisticated streaming applications in three simple steps: setup your streaming data sources, write your queries or streaming applications, and set up your destination for processed data. Kinesis Data Analytics cannot directly ingest data from the source as it ingests data either from Kinesis Data Streams or Kinesis Data Firehose, so this ↑ n is ruled out.

Ingest the data in AWS Glue job and use Spark transformations before writing to 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. AWS Glue job is meant to be used for batch ETL data processing and it's not the right fit for a near real-time data processing use-case.

Ingest the data in a Spark Streaming Cluster on EMR use Spark Streaming transformations before writing to S3 – Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. Amazon EMR uses Hadoop, an open-source framework, to distribute your data and processing across a resizable cluster of Amazon EC2 instances. Using an EMR cluster would imply managing the underlying infrastructure so it's ruled out because the correct solution for the given use-case should require the least amount of infrastructure maintenance.

Question 5:

A gaming company is developing a mobile game that streams score updates to a backend processor and then publishes results on a leaderboard. The company has hired you as an AWS Certified Solutions Architect Associate to design a solution that can handle major traffic spikes, process the mobile game updates in the order of receipt, and store the processed updates in a highly available database. The company wants to minimize the management overhead required to maintain the solution.

Which of the following will you recommend to meet these requirements?

Options:

- A. Push score updates to Kinesis Data Streams which uses a fleet of EC2 instances (with Auto Scaling) to process the updates in Kinesis Data Streams and then store these processed updates in DynamoDB
- B. Push score updates to an SNS topic, subscribe a Lambda function to this SNS topic to process the updates and then store these processed updates in a SQL database running on Amazon EC2
- C. Push score updates to Kinesis Data Streams which uses a Lambda function to process these updates and then store these processed updates in DynamoDB
- D. Push score updates to an SQS queue which uses a fleet of EC2 instances (with Auto Scaling) to process these updates in the SQS queue and then store these processed updates in an RDS MySQL database

Answer: C

Explanation

Correct option:

Push score updates to Kinesis Data Streams which uses a Lambda function to process these updates and then store these processed updates in DynamoDB

To help ingest real-time data or streaming data at large scales, you can use Amazon Kinesis Data Streams (KDS). KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources. The data collected is available in milliseconds, enabling real-time analytics. KDS provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications.

Lambda integrates natively with Kinesis Data Streams. The polling, checkpointing, and error handling complexities are abstracted when you use this native integration. The processed data can then be configured to be saved in DynamoDB.

Incorrect options:

Push score updates to an SQS queue which uses a fleet of EC2 instances (with Auto Scaling) to process these updates in the SQS queue and then store these processed updates in an RDS MySQL database

Push score updates to Kinesis Data Streams which uses a fleet of EC2 instances (with Auto Scaling) to process the updates in Kinesis Data Streams and then store these processed updates in DynamoDB

Push score updates to an SNS topic, subscribe a Lambda function to this SNS topic to process the updates, and then store these processed updates in a SQL database running on Amazon EC2

These three options use EC2 instances as part of the solution architecture. The use-case seeks to minimize the management overhead required to maintain the solution. However, EC2 instances involve several maintenance activities such as managing the guest operating system and software deployed to the guest operating system, including updates and security patches, etc. Hence these options are incorrect.

Question 6:

A telecom company operates thousands of hardware devices like switches, routers, cables, etc. The real-time status data for these devices must be fed into a communications application for notifications. Simultaneously, another analytics application needs to read the same real-time status data and analyze all the connecting lines that may go down because of any device failures.

As a Solutions Architect, which of the following solutions would you suggest, so that both the applications can connect to the real-time status data concurrently?

Options:

- A. Amazon Kinesis Data Streams
- B. Amazon Simple Notification Service (SNS)
- C. Amazon Simple Queue Service (SQS) with Amazon Simple Notification Service (SNS)
- D. Amazon Simple Queue Service (SQS) with Amazon Simple Email Service (Amazon SES)

Answer: A**Explanation****Correct option:**

Amazon Kinesis Data Streams – Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering).

AWS recommends Amazon Kinesis Data Streams for use cases with requirements that are similar to the following:

Routing related records to the same record processor (as in streaming MapReduce). For example, counting and aggregation are simpler when all records for a given key are routed to the same record processor.

Ordering of records. For example, you want to transfer log data from the application host to the processing/archival host while maintaining the order of log statements.

Ability for multiple applications to consume the same stream concurrently. For example, you have one application that updates a real-time dashboard and another that archives data to Amazon Redshift. You want both applications to consume data from the same stream concurrently and independently.

Ability to consume records in the same order a few hours later. For example, you have a billing application and an audit application that runs a few hours behind the billing application. Because Amazon Kinesis Data Streams stores data for up to 7 days, you can run the audit application up to 7 days behind the billing application.

Incorrect options:

Amazon Simple Notification Service (SNS) – Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging. SNS is a notification service and cannot be used for real-time processing of data.

Amazon Simple Queue Service (SQS) with Amazon Simple Notification Service (SNS) – Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows. Since multiple applications need to consume the same data stream concurrently, Kinesis is a better choice when compared to the combination of SQS with SNS.

Amazon Simple Queue Service (SQS) with Amazon Simple Email Service (Amazon SES) – As discussed above, Kinesis is a better option for this use case in comparison to SQS. Also, SES does not fit this use-case. Hence, this option is an incorrect answer.

Question 36:

An IT company is working on client engagement to build a real-time data analytics tool for the Internet of Things (IoT) data. The IoT data is funneled into Kinesis Data Streams which further acts as the source of a delivery stream for Kinesis Firehose. The engineering team has now configured a Kinesis Agent to send IoT data from another set of devices to the same Firehose delivery stream. They noticed that data is not reaching Firehose as expected.

As a solutions architect, which of the following options would you attribute as the MOST plausible root cause behind this issue?

- A• Kinesis Firehose delivery stream has reached its limit and needs to be scaled manually
- B• The data sent by Kinesis Agent is lost because of a configuration error
- C• Kinesis Agent can only write to Kinesis Data Streams, not to Kinesis Firehose
- D• Kinesis Agent cannot write to a Kinesis Firehose for which the delivery stream source is already set as Kinesis Data Streams

Answer: D**Explanation****Correct option:**

**Kinesis Agent cannot write to a Kinesis Firehose for which the delivery stream source is already set as Kinesis Data

Amazon Kinesis Data Firehose is the easiest way to reliably load streaming data into data lakes, data stores, and a  analytics tools. It is a fully managed service that automatically scales to match the throughput of your data and requires minimal ongoing administration. It can also batch, compress, transform, and encrypt the data before loading it, minimizing the amount of storage

used at the destination and increasing security.

When a Kinesis data stream is configured as the source of a Firehose delivery stream, Firehose's PutRecord and PutRecordBatch operations are disabled and Kinesis Agent cannot write to Firehose delivery stream directly. Data needs to be added to the Kinesis data stream through the Kinesis Data Streams PutRecord and PutRecords operations instead. Therefore, this option is correct.

Incorrect options:

Kinesis Agent can only write to Kinesis Data Streams, not to Kinesis Firehose – Kinesis Agent is a stand-alone Java software application that offers an easy way to collect and send data to Kinesis Data Streams or Kinesis Firehose. So this option is incorrect.

Kinesis Firehose delivery stream has reached its limit and needs to be scaled manually – Kinesis Firehose is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. Therefore this option is not correct.

The data sent by Kinesis Agent is lost because of a configuration error – This is a made-up option and has been added as a distractor.

101. Web Identity Federation – Cognito

Question 1:

You are building a mobile application. The security requirement for this application is that each user access it with MFA authentication.

Choose a method that meets this requirement.

Options:

- A. Set up IAM policies for customer accounts to enable MFA authentication
- B. Implement MFA functionality by integrating API Gateway, Lambda functions and SNS
- C. Implement mobile authentication using AWS Cognito
- D. Implement MFA authentication function by CloudHSM

Answer: C

Explanation

Option 3 is the correct answer. You can use Amazon Cognito to implement the authentication function of your application. With Amazon Cognito, you can add multi-factor authentication and encryption of stored and transferred data to your mobile application. You can also implement sign-in capabilities using social identity providers such as Google, Facebook, and Amazon, and enterprise identity providers such as Microsoft Active Directory with SAML.

Option 1 is incorrect. IAM policy is a service for user management within AWS and cannot be used as a customer management function of the application.

Option 2 is incorrect. You can't implement MFA using API Gateway or Lambda functions.

Option 4 is incorrect. CloudHSM is a cloud-based hardware security module (HSM). This makes it easy to generate and use encryption keys in the AWS cloud. It has nothing to do with MFA verification.

Question 12: Skipped

You have been hired as a Solutions Architect to advise a company on the various authentication/authorization mechanisms that AWS offers to authorize an API call within the API Gateway. The company would prefer a solution that offers built-in user management.

Which of the following solutions would you suggest as the best fit for the given use-case?

- Use Amazon Cognito User Pools (Correct)
- Use Amazon Cognito Identity Pools
- Use AWS_IAM authorization
- Use API Gateway Lambda authorizer

Explanation

Correct option:

Use Amazon Cognito User Pools – A user pool is a user directory in Amazon Cognito. You can leverage Amazon Cognito User Pools to either provide built-in user management or integrate with external identity providers, such as Facebook, Twitter, Google+, and Amazon. Whether your users sign-in directly or through a third party, all members of the user pool have a directc ↑ ofile that you can access through a Software Development Kit (SDK).

User pools provide: 1. Sign-up and sign-in services. 2. A built-in, customizable web UI to sign in users. 3. Social sign-in with Facebook, Google, Login with Amazon, and Sign in with Apple, as well as sign-in with SAML identity providers from your user pool. 4. User directory management and user profiles. 5. Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification. 6. Customized workflows and user migration through AWS Lambda triggers.

After creating an Amazon Cognito user pool, in API Gateway, you must then create a COGNITO_USER_POOLS authorizer that uses the user pool.

Incorrect options:

Use AWS_IAM authorization – For consumers who currently are located within your AWS environment or have the means to retrieve AWS Identity and Access Management (IAM) temporary credentials to access your environment, you can use AWS_IAM authorization and add least-privileged permissions to the respective IAM role to securely invoke your API. API Gateway API Keys is not a security mechanism and should not be used for authorization unless it's a public API. It should be used primarily to track a consumer's usage across your API.

Use API Gateway Lambda authorizer – If you have an existing Identity Provider (IdP), you can use an API Gateway Lambda authorizer to invoke a Lambda function to authenticate/validate a given user against your IdP. You can use a Lambda authorizer for custom validation logic based on identity metadata.

A Lambda authorizer can send additional information derived from a bearer token or request context values to your backend service. For example, the authorizer can return a map containing user IDs, user names, and scope. By using Lambda authorizers, your backend does not need to map authorization tokens to user-centric data, allowing you to limit the exposure of such information to just the authorization function.

When using Lambda authorizers, AWS strictly advises against passing credentials or any sort of sensitive data via query string parameters or headers, so this is not as secure as using Cognito User Pools.

In addition, both these options do not offer built-in user management.

Use Amazon Cognito Identity Pools – The two main components of Amazon Cognito are user pools and identity pools. Identity pools provide AWS credentials to grant your users access to other AWS services. To enable users in your user pool to access AWS resources, you can configure an identity pool to exchange user pool tokens for AWS credentials. So, identity pools aren't an authentication mechanism in themselves and hence aren't a choice for this use case.

Question 31:

A social media application is hosted on an EC2 server fleet running behind an Application Load Balancer. The application traffic is fronted by a CloudFront distribution. The engineering team wants to decouple the user authentication process for the application, so that the application servers can just focus on the business logic.

As a Solutions Architect, which of the following solutions would you recommend to the development team so that it requires minimal development effort?

- A• Use Cognito Authentication via Cognito Identity Pools for your CloudFront distribution
- B• Use Cognito Authentication via Cognito User Pools for your CloudFront distribution
- C• Use Cognito Authentication via Cognito Identity Pools for your Application Load Balancer
- D• Use Cognito Authentication via Cognito User Pools for your Application Load Balancer

Answer: D

Explanation

Correct option:

Use Cognito Authentication via Cognito User Pools for your Application Load Balancer

Application Load Balancer can be used to securely authenticate users for accessing your applications. This enables you to offload the work of authenticating users to your load balancer so that your applications can focus on their business logic. You can use Cognito User Pools to authenticate users through well-known social IdPs, such as Amazon, Facebook, or Google, through the user pools supported by Amazon Cognito or through corporate identities, using SAML, LDAP, or Microsoft AD, through the user pools supported by Amazon Cognito. You configure user authentication by creating an authenticate action for one or more listener rules.

Incorrect options:

Use Cognito Authentication via Cognito Identity Pools for your Application Load Balancer – There is no such thing as using Cognito Authentication via Cognito Identity Pools for managing user authentication for the application. Application-specific user authentication can be provided via Cognito User Pools. Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token.

Use Cognito Authentication via Cognito User Pools for your CloudFront distribution – You cannot directly integrate Cognito User

Pools with CloudFront distribution as you have to create a separate Lambda@Edge function to accomplish the authentication via Cognito User Pools. This involves additional development effort, so this option is not the best fit for the given use-case.

Use Cognito Authentication via Cognito Identity Pools for your CloudFront distribution – You cannot use Cognito Identity Pools for managing user authentication, so this option is not correct.

102. Reducing Security Threats

103. Key Management Service (KMS)

Question 1:

A US-based healthcare startup is building an interactive diagnostic tool for COVID-19 related assessments. The users would be required to capture their personal health records via this tool. As this is sensitive health information, the backup of the user data must be kept encrypted in S3. The startup does not want to provide its own encryption keys but still wants to maintain an audit trail of when an encryption key was used and by whom.

Which of the following is the BEST solution for this use-case?

Options:

- A. Use SSE-KMS to encrypt the user data on S3
- B. Use SSE-S3 to encrypt the user data on S3
- C. Use SSE-C to encrypt the user data on S3
- D. Use client-side encryption with client provided keys and then upload the encrypted user data to S3

Answer: A

Explanation

Correct option:

Use SSE-KMS to encrypt the user data on S3

AWS Key Management Service (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud. When you use server-side encryption with AWS KMS (SSE-KMS), you can specify a customer-managed CMK that you have already created. SSE-KMS provides you with an audit trail that shows when your CMK was used and by whom. Therefore SSE-KMS is the correct solution for this use-case.

Incorrect options:

Use SSE-S3 to encrypt the user data on S3 – When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. However this option does not provide the ability to audit trail the usage of the encryption keys.

Use SSE-C to encrypt the user data on S3 – With Server-Side Encryption with Customer-Provided Keys (SSE-C), you manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption when you access your objects. However this option does not provide the ability to audit trail the usage of the encryption keys.

Use client-side encryption with client provided keys and then upload the encrypted user data to S3 – Using client-side encryption is ruled out as the startup does not want to provide the encryption keys.

Question 14: Skipped

A financial services company has developed its flagship application on AWS Cloud with data security requirements such that the encryption key must be stored in a custom application running on-premises. The company wants to offload the data storage as well as the encryption process to Amazon S3 but continue to use the existing encryption key.

Which of the following S3 encryption options allows the company to leverage Amazon S3 for storing data with given constraints?

- Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)
- Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- Client-Side Encryption with data encryption is done on the client-side before sending it to Amazon S3
- Server-Side Encryption with Customer-Provided Keys (SSE-C)(Correct)

Explanation

Correct option:

Server-Side Encryption with Customer-Provided Keys (SSE-C)

You have the following options for protecting data at rest in Amazon S3:

Server-Side Encryption – Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects.

Client-Side Encryption – Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

For the given use-case, the company wants to manage the encryption keys via its custom application and let S3 manage the encryption, therefore you must use Server-Side Encryption with Customer-Provided Keys (SSE-C).

Incorrect options:

Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) – When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. So this option is incorrect.

Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) – Server-Side Encryption with Customer Master Keys (CMKs) stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3. SSE-KMS provides you with an audit trail that shows when your CMK was used and by whom. Additionally, you can create and manage customer-managed CMKs or use AWS managed CMKs that are unique to you, your service, and your Region.

Client-Side Encryption with data encryption is done on the client-side before sending it to Amazon S3 – You can encrypt the data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

104. Cloud HSM

105. Parameter Store

106. Lambda

Question 1:

Currently, as a Solutions Architect, you are designing the architecture of your application using AWS services. This application is virtually stateless and you want to build a cost-optimal application. You also want to add the ability to expand based on processing power needs.

Which AWS service should you choose to meet this requirement?

Options:

- A. Lambda
- B. DynamoDB
- C. Kinesis
- D. EC2

Answer: A

Explanation

A stateless application is an application that does not require information of the client's state to be communicated constantly in the system and does not retain session information each time. Therefore, the application will provide the same response to all end users when the same input is given. It will respond as if it were the clients first session each time. Lambda functions can achieve stateless application processing cost-optimally. Therefore, option 1 is the correct answer.

Option 2 is incorrect. DynamoDB is a NoSQL type DB and is used for high-speed and simple database processing. It can be used for serverless data processing linked with Lambda functions, but it is not correct because it is not a service for stateless application development. Rather, DynamoDB is used to store session data.

Option 3 is incorrect. Kinesis is a service used for processing and analysis of streaming data. It is not correct because it is not a service for stateless application development.

Option 4 is incorrect. It is possible to build stateless applications using EC2 instances. However, it is not a cost-optimal application compared to a serverless application that uses Lambda functions.

Question 2:

A solutions architect is designing a new service that will use an Amazon API Gateway API on the frontend. The service will need to persist data in a backend database using key-value requests. Initially, the data requirements will be around 1 MB and future growth is unknown. Requests can range from 0 to over 800 requests per second.

Which combination of AWS services would meet these requirements? (Select TWO.)

Options:

- A. Fargate
- B. Lambda
- C. RDS
- D. EC2 Auto Scaling
- E. Dynamo DB

Answer: B & E

Explanation

In this case AWS Lambda can perform the computation and store the data in an Amazon DynamoDB table. Lambda can scale concurrent executions to meet demand easily and DynamoDB is built for key-value data storage requirements and is also serverless and easily scalable. This is therefore a cost effective solution for unpredictable workloads.

CORRECT: “AWS Lambda” is a correct answer.

CORRECT: “Amazon DynamoDB” is also a correct answer.

INCORRECT: “AWS Fargate” is incorrect as containers run constantly and therefore incur costs even when no requests are being made.

INCORRECT: “Amazon EC2 Auto Scaling” is incorrect as this uses EC2 instances which will incur costs even when no requests are being made.

INCORRECT: “Amazon RDS” is incorrect as this is a relational database not a No-SQL database. It is therefore not suitable for key-value data storage requirements.

Question 3:

An IT Company wants to move all the compute components of its AWS Cloud infrastructure into serverless architecture. Their development stack comprises a mix of backend programming languages and the company would like to explore the support offered by the AWS Lambda runtime for their programming languages stack.

Can you identify the programming languages supported by the Lambda runtime? (Select two)

Options:

- A. C
- B. C#/ .NET
- C. PHP
- D. Go
- E. R

Answer: B & D

Explanation

Correct options:

C#/.NET

Go

A runtime is a version of a programming language or framework that you can use to write Lambda functions. AWS Lambda supports runtimes for the following languages:

C#/.NET

Go

Java

Node.js

Python

Ruby

Incorrect options:

C

PHP

R

Given the list of supported runtimes above, these three options are incorrect.

107. Build a Serverless Webpage with API Gateway and Lambda

108. Build an Alexa Skill

109. Serverless Application Model (SAM)

110. Elastic Container Service (ECS)

Question 1:

Your company decided to use Amazon ECS to set up a Docker container-based CI / CD environment on AWS. You are in charge of building this environment as a solutions architect. The requirement requested by your boss is to have a minimal spent on configuration when starting the container.

Choose how to set up ECS to achieve this requirement.

Options:

- A. Select the auto scaling launch type in ECS
- B. Select the Fargate launch type in ECS
- C. Select the EC2 launch type in ECS
- D. Select the Chef launch type in ECS

Answer: B

Explanation

The launch type of Amazon ECS determines the type of infrastructure in which tasks and services are hosted. And you can choose from two types, Fargate startup type and EC2 startup type.

The Fargate launch type allows you to run containerized applications without having to provision and manage your backend infrastructure. Simply register the task definition and Fargate will start the container. This configuration eliminates the need for tedious instance setup to launch a container. Therefore, option 2 is the correct answer.

Option 3 is incorrect. The EC2 launch type allows you to run containerized applications on a cluster of Amazon EC2 instances that you manage. It is an incorrect answer because it is a startup type that requires EC2 settings and does not meet the requirements.

Options 1 and 4 are incorrect because there are no other activation types.

Question 2:

An application running on an Amazon ECS container instance using the EC2 launch type needs permissions to write data to Amazon DynamoDB.

How can you assign these permissions only to the specific ECS task that is running the application?

Options:

- A. Modify the AmazonECSTaskExecutionRolePolicy policy to add permissions for DynamoDB
- B. Create an IAM policy with permissions to DynamoDB and assign It to a task using the taskRoleArn parameter
- C. Use a security group to allow outbound connections to DynamoDB and assign it to the container instance
- D. Create an IAM policy with permissions to DynamoDB and attach it to the container instance

Answer: B

Explanation

To specify permissions for a specific task on Amazon ECS you should use IAM Roles for Tasks. The permissions policy can be applied to tasks when creating the task definition, or by using an IAM task role override using the AWS CLI or SDKs. The taskRoleArn parameter is used to specify the policy.

CORRECT: “Create an IAM policy with permissions to DynamoDB and assign It to a task using the taskRoleArn parameter” is the correct answer.

INCORRECT: “Create an IAM policy with permissions to DynamoDB and attach it to the container instance” is incorrect. You should not apply the permissions to the container instance as they will then apply to all tasks running on the instance as well as the instance itself.

INCORRECT: “Use a security group to allow outbound connections to DynamoDB and assign it to the container instance” is incorrect. Though you will need a security group to allow outbound connections to DynamoDB, the question is asking how to assign permissions to write data to DynamoDB and a security group cannot provide those permissions.

INCORRECT: “Modify the AmazonECSTaskExecutionRolePolicy policy to add permissions for DynamoDB” is incorrect. The AmazonECSTaskExecutionRolePolicy policy is the Task Execution IAM Role. This is used by the container agent to pull container images, write log file etc.

Question 3:

A leading social media analytics company is contemplating moving its dockerized application stack into AWS Cloud. The company is not sure about the pricing for using Elastic Container Service (ECS) with the EC2 launch type compared to the Elastic Container Service (ECS) with the Fargate launch type.

Which of the following is correct regarding the pricing for these two services?

Options:

- A. Both ECS with EC2 launch type and ECS with Fargate launch type are charged based on vCPU and memory resources that the containerized application requests
- B. Both ECS with EC2 launch type and ECS with Fargate launch type are charged based on EC2 instances and EBS volumes used
- C. ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests
- D. Both ECS with EC2 launch type and ECS with Fargate launch type are just charged based on Elastic Container Service used per hour

Answer: C

Explanation

Correct option:

ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests

Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service. ECS allows you to easily run, scale, and secure Docker container applications on AWS.

With the Fargate launch type, you pay for the amount of vCPU and memory resources that your containerized application requests. vCPU and memory resources are calculated from the time your container images are pulled until the Amazon ECS Task* terminates, rounded up to the nearest second. With the EC2 launch type, there is no additional charge for the EC2 launch type.

You pay for AWS resources (e.g. EC2 instances or EBS volumes) you create to store and run your application.

Incorrect options:

Both ECS with EC2 launch type and ECS with Fargate launch type are charged based on vCPU and memory resources that the containerized application requests

Both ECS with EC2 launch type and ECS with Fargate launch type are charged based on EC2 instances and EBS volumes used As mentioned above – with the Fargate launch type, you pay for the amount of vCPU and memory resources. With EC2 launch type, you pay for AWS resources (e.g. EC2 instances or EBS volumes). Hence both these options are incorrect.

Both ECS with EC2 launch type and ECS with Fargate launch type are just charged based on Elastic Container Service used per hour

This is a made-up option and has been added as a distractor.

111. Miscellaneous

Question 1:

Your company has a development system in which a production environment and a test environment are separately prepared on AWS. As a Solutions Architect, you are working on a stack-based deployment model of AWS resources. Different layers are needed for the application's server and database.

Choose the appropriate course of action that meets this requirement.

Options:

- A. Use OpsWorks to define a stack for each layer of your application
- B. Use CloudFormation to define a stack for each layer of your application
- C. Use CodePipeline to define a stack for each layer of your application
- D. Use Elastic Beanstalk to define a stack for each layer of your application

Answer: A

Explanation:

Option A is the correct answer. AWS OpsWorks Stacks allows you to manage your applications and servers on AWS and on-premises. OpsWorks Stacks allows you to model your application as a stack which contains various layers such as load distribution, databases, and application servers.

Option B is incorrect. In order to prepare different layers on a stack basis, it is preferable to make detailed settings in OpsWorks

rather than CloudFormation.

Option C is incorrect. CodePipeline is a fully managed, continuous delivery service that automates releases for fast and efficient updates of applications and infrastructure. CodePipeline cannot set application layers.

Option D is incorrect. Elastic Beanstalk is a service for deploying and versioning web applications and services developed using Java, .NET, PHP, Node.js, Python, Ruby, Go and Docker on servers such as Apache. Elastic Beanstalk cannot set application layer.

Question 2:

Company-A has EC2 instances hosted in two AZs in a single region and the web application is also has ELB and Auto-Scaling. The application needs database tier synchronization. If/when one AZ becomes unavailable, Auto Scaling will take time to launch a new instance in a remaining AZ. You have been asked to make appropriate adjustments so that this application still remains fully available, even during the time when Auto scaling is spinning up replacements instances.

Choose the architectural enhancements you need to meet these requirements.

Options:

- A. Deploy EC2 instances in 3 AZs with each AZ set to handle up to 50% peak load capacity
- B. Deploy EC2 instances in 3 AZs with each AZ set to handle up to 40% peak load capacity
- C. Deploy EC2 instances in 2 AZs, across 2 regions, with each AZ set to handle up to 50% peak load capacity
- D. Deploy EC2 instances in 2 AZs with each AZ set to handle up to 50% peak load capacity

Answer: A

Explanation:

In this scenario, you need to maintain 100% availability as a requirement that the application never stops, even if one AZ were to go down. Therefore, it is necessary to choose a setting that can maintain 100% of the EC2 instance's peak load, even if one AZ becomes unavailable. If you deploy your EC2 instances over 3 AZ, each set with the ability to handle 50% peak load, you can maintain 100% even if one AZ goes down.

Therefore, option 1 is the correct answer.

Option 2 is incorrect because it will operate at 80% availability instead of the 100% availability required if one AZ goes down.

This question requires that the ability to handle peak load for instances does not fall below 100%, even if one AZ falls. Although it is possible to recover the peak load over time via Auto Scaling, there will still be a short time when the peak load cannot be appropriately processed. Then, in order to maintain 100% capacity to handle peak load, you need a current processing capacity exceeding 100%, (by enough to offset the losses due to AZ failure) until you can restore the processing capacity with Auto Scaling.

Options 3 and 4 are incorrect as the two AZs cannot achieve 100% availability if one AZ were to go down. They would only handle up to 50%.

Question 3:

Your customer wants to import an existing virtual machine into the AWS cloud. As a Solutions Architect, you have decided to consider a migration method.

Which service should you use?

Options:

- A. AWS Import/ Export
- B. VM Import/ Export
- C. Direct Connect
- D. VPC Peering

Answer: B

Explanation:

VM Import / Export allows you to import virtual machine (VM) images from your existing virtualized environment into Amazon EC2. You can use this service to migrate applications and workloads to Amazon EC2, copy VM image catalog to Amazon EC2, and create VM image repositories for backup and disaster recovery.

Other services are incorrect because they are not available to import existing virtual machines into the AWS cloud.

Option 1 is incorrect. AWS Import / Export is a service that you can use to transfer large amounts of data from your physical storage device to AWS. This is not appropriate because it is not used to import existing virtual machines into the AWS cloud.

Option 3 is incorrect. Direct connect is a dedicated line service that connects your on-premises environment to your VPC. This is incorrect because it is not used to import existing virtual machines into the AWS cloud.

Option 4 is incorrect. VPC peering is a function that connects two VPCs. This is incorrect because it is not used to import existing virtual machines into the AWS cloud.

Question 4:

As a Solutions Architect, you plan to move your infrastructure to the AWS cloud. I want to take advantage of the Chef recipes you are currently using to manage the configuration of your infrastructure.

Which AWS service is best for this requirement?

Options:

- A. Elastic Beanstalk
- B. OpsWorks
- C. CloudFormation
- D. ECS

Answer: B

Explanation

Option 2 is the correct answer. With AWS OpsWorks, you can leverage Chef to deploy your infrastructure on AWS. AWS OpsWorks is an environment automation service that uses Puppet or Chef to set up and operate applications in a cloud environment. OpsWorks Stacks and OpsWorks for Chef Automate allow you to use Chef cookbooks and solutions for configuration management.

Option 1 is incorrect. Elastic Beanstalk is used for deploying web applications and does not use Chef.

Option 3 is incorrect. CloudFormation is a tool that automates AWS resource deployment with JSON / YAML. This also doesn't use Chef.

Option 4 is incorrect. ECS is a container orchestration service that uses Docker. This also doesn't use Chef.

Question 5:

As a Solutions Architect, you develop and test your applications on AWS. In doing so, we want to provision the test environment quickly and make it easy to remove.

Choose the best AWS service settings to meet this requirement.

Options:

- A. Setting CodePipeline enables quick configuration and deletion
- B. Use CloudFormation template for creating a test environment
- C. Automate environment construction using AMI and Bash script of EC2 instance
- D. Setting ECR allows for quick configuration and deletion

Answer: B

Explanation

You can use CloudFormation templates to provision AWS resources with constant settings at all times. This makes it easy to create an environment like a test environment. Option 2 is the correct answer.

Option 1 is incorrect. CodePipeline automates the release step by configuring services like CodeDeploy and ECS as a pipeline. CodePipeline needs to use other services such as CloudFormation to set up the infrastructure environment.

Option 3 is incorrect. AMI and Bash are settings limited to EC2 instances and cannot be used to automate overall infrastructure construction.

Option 4 is incorrect. ECR is a service that saves a file called a Docker image.

Question 6:

An AWS Organization has an OU with multiple member accounts in it. The company needs to restrict the ability to launch only specific Amazon EC2 instance types. How can this policy be applied across the accounts with the least effort?

Options:

- A. Use AWS Resource Access Manager to control which launch types can be used
- B. Create an SCP with an allow rule that allows launching the specific instance types
- C. Create an IAM policy to deny launching all but the specific instance types
- D. Create an SCP with a deny rule that denies all but the specific instance types

Answer: D

Explanation

To apply the restrictions across multiple member accounts you must use a Service Control Policy (SCP) in the AWS Organization. The way you would do this is to create a deny rule that applies to anything that does not equal the specific instance type you want to allow.

CORRECT: "Create an SCP with a deny rule that denies all but the specific instance types" is the correct answer.

INCORRECT: "Create an SCP with an allow rule that allows launching the specific instance types" is incorrect as any rule is required.

INCORRECT: “Create an IAM policy to deny launching all but the specific instance types” is incorrect. With IAM you need to apply the policy within each account rather than centrally so this would require much more effort.

INCORRECT: “Use AWS Resource Access Manager to control which launch types can be used” is incorrect. AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. It is not used for restricting access or permissions.

Question 7:

A web application runs in public and private subnets. The application architecture consists of a web tier and database tier running on Amazon EC2 instances. Both tiers run in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

Options:

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

Answer: A & B

Explanation

To add high availability to this architecture both the web tier and database tier require changes. For the web tier an Auto Scaling group across multiple AZs with an ALB will ensure there are always instances running and traffic is being distributed to them.

The database tier should be migrated from the EC2 instances to Amazon RDS to take advantage of a managed database with Multi-AZ functionality. This will ensure that if there is an issue preventing access to the primary database a secondary database can take over.

CORRECT: “Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs” is the correct answer.

CORRECT: “Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment” is the correct answer.

INCORRECT: “Create new public and private subnets in the same AZ for high availability” is incorrect as this would not add high availability.

INCORRECT: “Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)” is incorrect because the existing servers are in a single subnet. For HA we need to instances in multiple subnets.

INCORRECT: “Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ” is incorrect because we also need HA for the database layer.

Question 9:

An eCommerce company runs an application on Amazon EC2 instances in public and private subnets. The web application runs in a public subnet and the database runs in a private subnet. Both the public and private subnets are in a single Availability Zone.

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

Options:

- A. Create new public and private subnets in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment
- B. Create an EC2 Auto Scaling group and Application Load Balancer that spans across multiple AZs
- C. Create new public and private subnets in the same AZ but in a different Amazon VPC” is incorrect
- D. Create an EC2 Auto Scaling group in the public subnet and use an Application Load Balancer
- E. Create new public and private subnets in a different AZ. Create a database using Amazon EC2 in one AZ

Answer: A & B

Explanation

High availability can be achieved by using multiple Availability Zones within the same VPC. An EC2 Auto Scaling group can then be used to launch web application instances in multiple public subnets across multiple AZs and an ALB can be used to distribute incoming load.

The database solution can be made highly available by migrating from EC2 to Amazon RDS and using a Multi-AZ deployment model. This will provide the ability to failover to another AZ in the event of a failure of the primary database or the ↑ in which it runs.

CORRECT: “Create an EC2 Auto Scaling group and Application Load Balancer that spans across multiple AZs” is a correct answer.

CORRECT: “Create new public and private subnets in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment” is also a correct answer.

INCORRECT: “Create new public and private subnets in the same AZ but in a different Amazon VPC” is incorrect. You cannot use multiple VPCs for this solution as it would be difficult to manage and direct traffic (you can't load balance across VPCs).

INCORRECT: “Create an EC2 Auto Scaling group in the public subnet and use an Application Load Balancer” is incorrect. This does not achieve HA as you need multiple public subnets across multiple AZs.

INCORRECT: “Create new public and private subnets in a different AZ. Create a database using Amazon EC2 in one AZ” is incorrect. The database solution is not HA in this answer option.

Question 10:

A company uses Docker containers for many application workloads in an on-premise data center. The company is planning to deploy containers to AWS and the chief architect has mandated that the same configuration and administrative tools must be used across all containerized environments. The company also wishes to remain cloud agnostic to safeguard mitigate the impact of future changes in cloud strategy.

How can a Solutions Architect design a managed solution that will align with open-source software?

Options:

- A. Launch the containers on Amazon Elastic Kubernetes Service (EKS) and EKS worker nodes
- B. Launch the containers on a fleet of Amazon EC2 instances in a cluster placement group
- C. Launch the containers on Amazon Elastic Container Service (ECS) with AWS Fargate instances
- D. Launch the containers on Amazon Elastic Container Service (ECS) with Amazon EC2 instance worker nodes

Answer: A

Explanation

Amazon EKS is a managed service that can be used to run Kubernetes on AWS. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications. Applications running on Amazon EKS are fully compatible with applications running on any standard Kubernetes environment, whether running in on-premises data centers or public clouds. This means that you can easily migrate any standard Kubernetes application to Amazon EKS without any code modification.

This solution ensures that the same open-source software is used for automating the deployment, scaling, and management of containerized applications both on-premises and in the AWS Cloud.

CORRECT: “Launch the containers on Amazon Elastic Kubernetes Service (EKS) and EKS worker nodes” is the correct answer.

INCORRECT: “Launch the containers on a fleet of Amazon EC2 instances in a cluster placement group” is incorrect

INCORRECT: “Launch the containers on Amazon Elastic Container Service (ECS) with AWS Fargate instances” is incorrect

INCORRECT: “Launch the containers on Amazon Elastic Container Service (ECS) with Amazon EC2 instance worker nodes” is incorrect

Question 11:

A recent security audit uncovered some poor deployment and configuration practices within your VPC. You need to ensure that applications are deployed in secure configurations.

How can this be achieved in the most operationally efficient manner?

Options:

- A. Remove the ability for staff to deploy applications
- B. Use AWS Inspector to apply secure configurations
- C. Use CloudFormation with securely configured templates
- D. Manually check all application configurations before deployment

Answer: C

Explanation

CloudFormation helps users to deploy resources in a consistent and orderly way. By ensuring the CloudFormation templates are created and administered with the right security configurations for your resources, you can then repeatedly deploy resources with secure settings and reduce the risk of human error.

CORRECT: “Use CloudFormation with securely configured templates” is the correct answer.

INCORRECT: “Remove the ability for staff to deploy applications” is incorrect. Removing the ability of staff to deploy resources does not help you to deploy applications securely as it does not solve the problem of how to do this in an operationally efficient manner.

INCORRECT: “Manually check all application configurations before deployment” is incorrect. Manual checking of all application

configurations before deployment is not operationally efficient.

INCORRECT: “Use AWS Inspector to apply secure configurations” is incorrect. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It is not used to secure the actual deployment of resources, only to assess the deployed state of the resources.

Question 12:

A Solutions Architect has been tasked with re-deploying an application running on AWS to enable high availability. The application processes messages that are received in an ActiveMQ queue running on a single Amazon EC2 instance. Messages are then processed by a consumer application running on Amazon EC2. After processing the messages the consumer application writes results to a MySQL database running on Amazon EC2.

Which architecture offers the highest availability and low operational complexity?

Options:

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

Answer: C

Explanation

The correct answer offers the highest availability as it includes Amazon MQ active/standby brokers across two AZs, an Auto Scaling group across two AZs and a Multi-AZ Amazon RDS MySQL database deployment.

This architecture not only offers the highest availability it is also operationally simple as it maximizes the usage of managed services.

CORRECT: “Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Create an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use an Amazon RDS MySQL database with Multi-AZ enabled” is the correct answer.

INCORRECT: “Deploy a second Active MQ server to another Availability Zone. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone” is incorrect. This architecture does not offer the highest availability as it does not use Auto Scaling. It is also not the most operationally efficient architecture as it does not use AWS managed services.

INCORRECT: “Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone” is incorrect. This architecture does not use Auto Scaling for best HA or the RDS managed service.

INCORRECT: “Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled” is incorrect. This solution does not use Auto Scaling.

Question 13:

A retail company uses Amazon EC2 instances, API Gateway, Amazon RDS, Elastic Load Balancer and CloudFront services. To improve the security of these services, the Risk Advisory group has suggested a feasibility check for using the Amazon GuardDuty service.

Which of the following would you identify as data sources supported by GuardDuty?

Options:

- A. VPC Flow Logs, API Gateway logs, S3 access logs
- B. ELB logs, DNS logs, CloudTrail events
- C. VPC Flow Logs, DNS logs, CloudTrail events
- D. CloudFront logs, API Gateway logs, CloudTrail events

Answer: C

Explanation

Correct option:

VPC Flow Logs, DNS logs, CloudTrail events – Amazon GuardDuty is a threat detection service that continuously monitors for

malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats.

GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail events, Amazon VPC Flow Logs, and DNS logs.

With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

Incorrect options:

VPC Flow Logs, API Gateway logs, S3 access logs

ELB logs, DNS logs, CloudTrail events

CloudFront logs, API Gateway logs, CloudTrail events

These three options contradict the explanation provided above, so these options are incorrect.

Question 14:

A financial services company recently launched an initiative to improve the security of its AWS resources and it had enabled AWS Shield Advanced across multiple AWS accounts owned by the company. Upon analysis, the company has found that the costs incurred are much higher than expected.

Which of the following would you attribute as the underlying reason for the unexpectedly high costs for AWS Shield Advanced service?

Options:

- A. AWS Shield Advanced also covers AWS Shield Standard plan, thereby resulting in increased costs
- B. Savings Plans has not been enabled for the AWS Shield Advanced service across all the AWS accounts
- C. Consolidated billing has not been enabled. All the AWS accounts should fall under a single consolidated billing for the monthly fee to be charged only once
- D. AWS Shield Advanced is being used for custom servers, that are not part of AWS Cloud, thereby resulting in increased costs

Answer: C

Explanation

Correct option:

Consolidated billing has not been enabled. All the AWS accounts should fall under a single consolidated billing for the monthly fee to be charged only once - If your organization has multiple AWS accounts, then you can subscribe multiple AWS Accounts to AWS Shield Advanced by individually enabling it on each account using the AWS Management Console or API. You will pay the monthly fee once as long as the AWS accounts are all under a single consolidated billing, and you own all the AWS accounts and resources in those accounts.

Incorrect options:

AWS Shield Advanced is being used for custom servers, that are not part of AWS Cloud, thereby resulting in increased costs - AWS Shield Advanced does offer protection to resources outside of AWS. This should not cause unexpected spike in billing costs.

AWS Shield Advanced also covers AWS Shield Standard plan, thereby resulting in increased costs - AWS Shield Standard is automatically enabled for all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service.

Savings Plans has not been enabled for the AWS Shield Advanced service across all the AWS accounts - This option has been added as a distractor. Savings Plans is a flexible pricing model that offers low prices on EC2, Lambda, and Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in \$/hour) for a 1 or 3 year term. Savings Plans is not applicable for the AWS Shield Advanced service.

Question 15:

A leading carmaker would like to build a new car-as-a-sensor service by leveraging fully serverless components that are provisioned and managed automatically by AWS. The development team at the carmaker does not want an option that requires the capacity to be manually provisioned, as it does not want to respond manually to changing volumes of sensor data.

Given these constraints, which of the following solutions is the BEST fit to develop this car-as-a-sensor service?

Options:

- A. Ingest the sensor data in a Kinesis Data Stream, which is polled by a Lambda function in batches, and the data is written into an auto-scaled DynamoDB table for downstream processing

- B. Ingest the sensor data in an Amazon SQS standard queue, which is polled by a Lambda function in batches and the data is written into an auto-scaled DynamoDB table for downstream processing
- C. Ingest the sensor data in an Amazon SQS standard queue, which is polled by an application running on an EC2 instance and the data is written into an auto-scaled DynamoDB table for downstream processing
- D. Ingest the sensor data in a Kinesis Data Stream, which is polled by an application running on an EC2 instance and the data is written into an auto-scaled DynamoDB table for downstream processing

Answer: B

Explanation

Correct option:

Ingest the sensor data in an Amazon SQS standard queue, which is polled by a Lambda function in batches and the data is written into an auto-scaled DynamoDB table for downstream processing

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

AWS manages all ongoing operations and underlying infrastructure needed to provide a highly available and scalable message queuing service. With SQS, there is no upfront cost, no need to acquire, install, and configure messaging software, and no time-consuming build-out and maintenance of supporting infrastructure. SQS queues are dynamically created and scale automatically so you can build and grow applications quickly and efficiently. As there is no need to manually provision the capacity, so this is the correct option.

Incorrect options:

Ingest the sensor data in a Kinesis Data Stream, which is polled by a Lambda function in batches, and the data is written into an auto-scaled DynamoDB table for downstream processing – Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. However, the user is expected to manually provision an appropriate number of shards to process the expected volume of the incoming data stream. The throughput of an Amazon Kinesis data stream is designed to scale without limits via increasing the number of shards within a data stream. Therefore Kinesis Data Streams is not the right fit for this use-case.

Ingest the sensor data in an Amazon SQS standard queue, which is polled by an application running on an EC2 instance and the data is written into an auto-scaled DynamoDB table for downstream processing

Ingest the sensor data in a Kinesis Data Stream, which is polled by an application running on an EC2 instance and the data is written into an auto-scaled DynamoDB table for downstream processing

Using an application on an EC2 instance is ruled out as the carmaker wants to use fully serverless components. So both these options are incorrect.

Question 16:

A financial services company uses Amazon GuardDuty for analyzing its AWS account metadata to meet the compliance guidelines. However, the company has now decided to stop using GuardDuty service. All the existing findings have to be deleted and cannot persist anywhere on AWS Cloud.

Which of the following techniques will help the company meet this requirement?

Options:

- A. Suspend the service in the general settings
- B. De-register the service under services tab
- C. Disable the service in the general settings
- D. Raise a service request with Amazon to completely delete the data from all their backups

Answer: C

Explanation

Correct option:

Amazon GuardDuty offers threat detection that enables you to continuously monitor and protect your AWS accounts, workloads, and data stored in Amazon S3. GuardDuty analyzes continuous streams of meta-data generated from your account network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.

Disable the service in the general settings – Disabling the service will delete all remaining data, including your findings and configurations before relinquishing the service permissions and resetting the service. So, this is the correct option for our use case.

Incorrect options:

Suspend the service in the general settings – You can stop Amazon GuardDuty from analyzing your data sources at any time by choosing to suspend the service in the general settings. This will immediately stop the service from analyzing data, but does not delete your existing findings or configurations.

De-register the service under services tab – This is a made-up option, used only as a distractor.

Raise a service request with Amazon to completely delete the data from all their backups – There is no need to create a service request as you can delete the existing findings by disabling the service.

Question 17:

An IT security consultancy is working on a solution to protect data stored in S3 from any malicious activity as well as check for any vulnerabilities on EC2 instances.

As a solutions architect, which of the following solutions would you suggest to help address the given requirement?

Options:

A. Use Amazon GuardDuty to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon GuardDuty to check for vulnerabilities on EC2 instances

B. Use Amazon GuardDuty to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon Inspector to check for vulnerabilities on EC2 instances

C. Use Amazon Inspector to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon Inspector to check for vulnerabilities on EC2 instances

D. Use Amazon Inspector to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon GuardDuty to check for vulnerabilities on EC2 instances

Answer: B

Explanation

Correct option:

Use Amazon GuardDuty to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon Inspector to check for vulnerabilities on EC2 instances

Amazon GuardDuty offers threat detection that enables you to continuously monitor and protect your AWS accounts, workloads, and data stored in Amazon S3. GuardDuty analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.

Amazon Inspector security assessments help you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.

Incorrect options:

Use Amazon GuardDuty to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon GuardDuty to check for vulnerabilities on EC2 instances

Use Amazon Inspector to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon Inspector to check for vulnerabilities on EC2 instances

Use Amazon Inspector to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon GuardDuty to check for vulnerabilities on EC2 instances

These three options contradict the explanation provided above, so these options are incorrect.

Question 16: Skipped

A big data consulting firm needs to set up a data lake on Amazon S3 for a Health-Care client. The data lake is split in raw and refined zones. For compliance reasons, the source data needs to be kept for a minimum of 5 years. The source data arrives in the raw zone and is then processed via an AWS Glue based ETL job into the refined zone. The business analysts run ad-hoc queries only on the data in the refined zone using AWS Athena. The team is concerned about the cost of data storage in both the raw and refined zones as the data is increasing at a rate of 1TB daily in each zone.

As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution? (Select t

- Create a Lambda function based job to delete the raw zone data after 1 day
- Setup a lifecycle policy to transition the refined zone data into Glacier Deep Archive after 1 day of object creation

- Use Glue ETL job to write the transformed data in the refined zone using a compressed file format (Correct)
- Use Glue ETL job to write the transformed data in the refined zone using CSV format
- Setup a lifecycle policy to transition the raw zone data into Glacier Deep Archive after 1 day of object creation(Correct)

Explanation

Correct options:

Setup a lifecycle policy to transition the raw zone data into Glacier Deep Archive after 1 day of object creation

You can manage your objects so that they are stored cost-effectively throughout their lifecycle by configuring their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

For the given use-case, the raw zone consists of the source data, so it cannot be deleted due to compliance reasons. Therefore, you should use a lifecycle policy to transition the raw zone data into Glacier Deep Archive after 1 day of object creation.

Use Glue ETL job to write the transformed data in the refined zone using a compressed file format

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. You cannot transition the refined zone data into Glacier Deep Archive because it is used by the business analysts for ad-hoc querying. Therefore, the best optimization is to have the refined zone data stored in a compressed format via the Glue job. The compressed data would reduce the storage cost incurred on the data in the refined zone.

Incorrect options:

Create a Lambda function based job to delete the raw zone data after 1 day – As mentioned in the use-case, the source data needs to be kept for a minimum of 5 years for compliance reasons. Therefore the data in the raw zone cannot be deleted after 1 day.

Setup a lifecycle policy to transition the refined zone data into Glacier Deep Archive after 1 day of object creation – You cannot transition the refined zone data into Glacier Deep Archive because it is used by the business analysts for ad-hoc querying. Hence this option is incorrect.

Use Glue ETL job to write the transformed data in the refined zone using CSV format – It is cost-optimal to write the data in the refined zone using a compressed format instead of CSV format. The compressed data would reduce the storage cost incurred on the data in the refined zone. So, this option is incorrect.

112

1. You are trying to launch an EC2 instance, however the instance seems to go into a terminated status immediately. What would probably not be a reason that this is happening?

- A. The AMI is missing the required part
- B. The snapshot is corrupt
- C. You need to create a storage in EBS first
- D. You have reached your volume limit.

Answer: C

2. In the context of AWS support, why must an EC2 instance be unreachable for 20 minutes rather than allowing customers to open tickets immediately.

- A. Because most reachability issues are resolved by automated processes in less than 20 mins
- B. Because all EC2 instances are unreachable for 20 min. every day when AWS does route maintenance
- C. Because all EC2 instances are unreachable for 20 mins when first launched
- D. Because of all the reasons listed here

Answer: A

Explanation: An EC2 instance must be unreachable for 20 mins before opening a ticket, because most reachability issues are resolved by automated processes in less than 20 mins and will not require any action on the part of the customer. If the instance is still unreachable after this time frame has passed, then you should open a case with support.

3. EBS provides the ability to create backups of any EC2 volume into what is known as

- A. Snapshots
- B. Images
- C. Instance backups
- D. Mirrors

Answer: A

Explanation: Amazon allows to make backups of the data stored in EBS volumes through snapshots that can later be used to create a new EBS volume.

4. A user is storing large number of objects on S3. The user wants to implement search functionality among the objects. How the user can achieve this?

- A. Use the indexing feature of S3
- B. Tag the objects with the metadata to search on that
- C. Use the query functionality of S3
- D. Make your own DB system which stores the S3 metadata for the search functionality.

Answer: D

Explanation: In AWS, S3 doesn't provide any query facility. To retrieve a specific object, the user needs to know the exact bucket/object key. In this case it is recommended to have an own DB system which manages the S3 metadata and key mapping.

5. After setting up a VPC network, a more experienced cloud engineer suggests that to achieve a low n/w latency and high n/w throughput you should look into setting up a placement group. You know nothing about this, but to begin to do some research about it and are especially curious about its limitations. Which of the below statements is wrong in describing the limitations of a placement group.

- A. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed.
- B. A placement group can span multiple AZs
- C. You cant move an existing instance into a placement group
- D. A placement group can span peered VPCs

Answer: B

A placement group is a logical grouping of instances within a single AZ. Using placement groups enables applications to participate in a low-latency, 10Gbps n/w. Placement groups are recommended for applications that benefit from low n/w latency, high n/w throughput, or both. To provide the lowest latency, and the highest packet-per-second n/w performance for your placement group, choose an instance type that supports enhanced networking. Placement groups have the following limitations: The name you specify for a placement group a name must be unique within your AWS account. A placement group cant span multiple AZs. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed. We recommend using the instance type for all instances in a placement group. You cant merge placement groups. Instead, you must terminate the instances in one placement group, and then relaunch those instances into the other placement groups. A placement group can span peered VPCs, however, you will not get full bisection bandwidth between instances in peered VPCs. You cant move an existing instance into a placement ↑ . You can create an AMI from an existing instance, and then launch a new instance from the AMI into a placement group.

6. What is a placement group in Amazon EC2?
- A. It is a group of EC2 instances within a single AZ
 - B. It is edge location of web content
 - C. It is the AWS region where you run the EC2 instance of web content
 - D. It is a group used to span multiple AZ

Answer: A

Explanation: A placement group is a logical grouping of instances within single AZ.

7. You are migrating an internal server of your DC to an EC2 instance with EBS volume. Your server disk usage is around 500 GB so you just copied all your data to a 2 TB disk to be used with AWS import/ export. Where will the data be imported once it arrives at Amazon.
- A. To a 2 TB EBS volume
 - B. To a S3 bucket with two objects of 1 TB
 - C. To 500 GB EBS volume
 - D. To S3 bucket as a 2 TB snapshot

Answer: B

Explanation: An import to EBS will have different results depending on whether the capacity of your storage device is <= 1 TB or > TB. The max size of EBS snapshot is 1 TB, so if the device image is larger than 1 TB, the image is chunked and stored on S3. The target location is determined based on the total capacity of the device, not the amount of data on the device.

8. A client needs you to import some existing infrastructure from a dedicated hosting provider to AWS to try and save on the cost of running his current website. He also needs an automated process that manages backups, s/w patching, automatic failure detection, and recovery. You are aware that his existing set up currently uses an Oracle DB. Which of the following AWS DBs could be best for accomplishing this task?
- A. Amazon RDS
 - B. Amazon Redshift
 - C. Amazon Simple DB
 - D. Amazon Elasti Cache

Answer: A

Explanation: Amazon RDS gives you access to the capabilities of a familiar MySQL, Oracle, SQL Server or Postgresql DB engine. This means that the code, applications, and tools that you are already use today with your existing DBs can be used with Amazon RDS. Amazon RDS automatically patches the DB s/w and backs up DB, storing the back ups for a user defined retention period and enabling point in time recovery.

9. True or False: A VPC contains multiple subnets, where each subnet can span multiple AZs
- A. True, only if requested during the setup of VPCs
 - B. True
 - C. False
 - D. True, only for US region.

Answer: C

Explanation: A VPC can span several AZs. In contrast a subnet must reside in a single AZ.
↑

10. A edge location refers to which Amazon web service.

- A. An edge location is referred to the n/w configured within a zone or region
- B. An edge location is referred to AWS region
- C. An edge location is the location of the data center used for Amazon cloud front
- D. An edge location is a zone within the AWS region

Answer: C

Explanation: Amazon cloud front is a content distributed n/w. A content delivery n/w or content distribution n/w (CDN) is a large distributed system of servers deployed in multiple data centers across the world. The location of the data center used for CDN is called edge location. Amazon cloud front can cache static content at each edge location. This means that your popular static content (ex: your sites logo, navigational images, CSS, JS code, etc) will be available at a nearby edge location for the browsers to download with low latency and improved performance for viewers. Caching popular static content with Cloud Front also helps you off load request for such files from your origin server. Cloud Front serves the cached copy when available and only makes a browser's request does not have a copy of the file.

10. You are looking at ways to improve some existing infrastructure as it seems a lot engineering resources are being taken up with basic management and monitoring tasks and the cost seems to be excessive. You are thinking of deploying Amazon Elasti Cache to help. Which of the following statements is true in regards to Elasti Cache.

- A. You can improve load and response time to user actions and queries. However the cost associated with scaling web application will be more.
- B. You can't improve load and response times to user actions and queries but you can reduce the cost associated with scaling web applications
- C. You can improve load and response times to user action and queries, however the cost associated with scaling web application will remain the same.
- D. You can improve load and response times to user actions and queries and also you can reduce the cost associated with scaling web applications

Answer: D

Explanation: Elasti Cache is a web service that makes it easy to deploy and run MemCached or Redis protocol compliant server nodes in the cloud. Elasti Cache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory caching system, instead of relying entirely on slower disk based DBs. The service simplifies and offloads the management, monitoring and operation of in-memory cache environments, enabling your engineering resources to focus on developing applications. Using Amazon Elasti Cache you can not only improve load and response times to user action and queries, but also reduce the cost associated with scaling web applications.

11. Your supervisor has asked to build a simple file synchronization service for your dept. He doesn't want to spend too much money and he wants to be notified of any changes to files by email. What do you think would be best amazon service to use for the email solution.

- A. Amazon SES (Simple Email Service)
- B. Amazon Cloud Search
- C. Amazon SWF (Simple Workflow Service)
- D. Amazon Appstream

Answer: A

Explanation: File change notifications can be sent via email to users following the resource with Amazon SES, an easy to use, cost effective email solution.

12. Your manager has just given access to multiple VPN connections that someone else has recently set up between all your company's offices. She needs you to make sure that the communication between VPN is secured. Which of the following services would be the best for providing a low-cost hub-and-scope model for primary and backup connectivity between these remote offices.

- A. Amazon Cloud Front
- B. AWS Direct Connect
- C. AWS Cloud HSM
- D. AWS VPN CloudHub

Answer: D

Explanation: If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. The VPN Cloud Hub operates on a simple hub-and-spoke mode that you can use with or w/o a VPC. This design is suitable for customers with multiple branch offices and existing internet connections who would like to implement a convenient, potentially low-cost hub-and-spoke model for primary or back up connectivity between these remote offices.

Pending first four

1. EC2 Compute - 42
2. Virtual Private Cloud - 46
3. Storage Services - 27
4. Security Architecture - 36
5. Database Services - 34
6. Fault Tolerant Systems - 19
7. Deployment and Orchestration - 33
8. Monitoring Services - 17

Total == 254

EC2 Compute

Question 1:

What three attributes are selectable when creating an EBS volume for an EC2 instance?

- A. volume type
- B. IOPS
- C. region
- D. CMK
- E. ELB
- F. EIP

Answer (A,B,D)

Question 2: You have been asked to migrate a 10 GB unencrypted EBS volume to an encrypted volume for security purposes. What are three key steps required as part of the migration?

- A. pause the unencrypted instance
- B. create a new encrypted volume of the same size and availability zone
- C. create a new encrypted volume of the same size in any availability zone
- D. start converter instance
- E. shutdown and detach the unencrypted instance

Answer (B,D,E)

Question 3: What is EC2 instance protection?

- A. prevents Auto Scaling from selecting specific EC2 instance to be replaced when scaling in
- B. prevents Auto Scaling from selecting specific EC2 instance to be

- replaced when scaling out
- C. prevents Auto Scaling from selecting specific EC2 instance for termination when scaling out
- D. prevents Auto Scaling from selecting specific EC2 instance for termination when scaling in
- E. prevents Auto Scaling from selecting specific EC2 instance for termination when paused
- F. prevents Auto Scaling from selecting specific EC2 instance for termination when stopped

Answer (D)

Question 4:

What two features are supported with EBS volume Snapshot feature?

- A. EBS replication across regions
- B. EBS multi-zone replication
- C. EBS single region only
- D. full snapshot data only
- E. unencrypted snapshot only

Answer (A,B)

Question 5:

What two resource tags are supported for an EC2 instance?

- A. VPC endpoint
- B. EIP
- C. network interface
- D. security group
- E. Flow Log

Answer (A,E)

Question 6:

What two options are available to alert tenants when an EC2 instance is terminated?

- A. SNS
- B. CloudTrail
- C. Lambda function
- D. SQS
- E. STS

Answer (A,C)

Question 7:

What class of EC2 instance type is recommended for running data analytics?

- A. memory optimized
- B. compute optimized
- C. storage optimized
- D. general purpose optimized

Answer (B)

Question 8:

What class of EC2 instance type is recommended for database servers?

- A. memory optimized
- B. compute optimized
- C. storage optimized
- D. general purpose optimized

Answer (A)

Question 9:

What two attributes distinguish each pricing model?

- A. reliability
- B. amazon service



- C. discount
- D. performance
- E. redundancy

Answer (A,C)

Question 10:

What are three standard AWS pricing models?

- A. elastic
- B. spot
- C. reserved
- D. dynamic
- E. demand

Answer (B,C,E)

Question 11:

How is an EBS root volume created when launching an EC2 instance from a new EBS-backed AMI?

- A. S3 template
- B. original AMI
- C. snapshot
- D. instance store

Answer (C)

Question 12:

What Amazon AWS sources are available for creating an EBS-Backed Linux AMI? (select two)

- A. EC2 instance
- B. Amazon SMS
- C. VM Import/Export
- D. EBS Snapshot
- E. S3 bucket

Answer (A,D)

Question 13:

What is required to prevent an instance from being launched and incurring costs?

- A. stop instance
- B. terminate instance
- C. terminate AMI and de-register instance
- D. stop and de-register instance
- E. stop, deregister AMI and terminate instance

Answer (E)

Question 14:

What is an EBS Snapshot?

- A. backup of an EBS root volume and instance data
- B. backup of an EC2 instance
- C. backup of configuration settings
- D. backup of instance store

Answer (A)

Question 15:

Where are ELB and Auto-Scaling groups deployed as a unified solution for horizontal scaling?

- A. database instances
- B. all instances
- C. web server instances
- D. default VPC only

Answer (C)

Question 16: What feature is supported when attaching or detaching an EBS



volume from an EC2 instance?

- A. EBS volume can be attached and detached to an EC2 instance in the same region
- B. EBS volume can be attached and detached to an EC2 instance that is cross-region
- C. EBS volume can only be copied and attached to an EC2 instance that is cross-region
- D. EBS volume can only be attached and detached to an EC2 instance in the same Availability Zone

Answer (D)

Question 17:

What two statements correctly describe how to add or modify IAM roles to a running EC2 instance?

- A. attach an IAM role to an existing EC2 instance from the EC2 console
- B. replace an IAM role attached to an existing EC2 instance from the EC2 console
- C. attach an IAM role to the user account and relaunch the EC2 instance
- D. add the EC2 instance to a group where the role is a member

Answer (A,B)

Question 18: What is the default behavior for an EC2 instance when terminated? (Select two)

- A. DeleteOnTermination attribute cannot be modified
- B. EBS root device volume and additional attached volumes are deleted immediately
- C. EBS data volumes that you attach at launch persist
- D. EBS root device volume is automatically deleted when instance terminates

Answer (C,D)

Question 19:

How do you launch an EC2 instance after it is terminated? (Select two)

- A. launch a new instance using the same AMI
- B. reboot instance from CLI
- C. launch a new instance from a Snapshot
- D. reboot instance from management console
- E. contact AWS support to reset

Answer (A,C)

Question 20:

What service can automate EBS snapshots (backups) for restoring EBS volumes?

- A. CloudWatch event
- B. SNS topic
- C. CloudTrail
- D. Amazon Inspector
- E. CloudWatch alarm

Answer (A)

Question 21:

What will cause AWS to terminate an EC2 instance on launch? (Select two)

- A. security group error
- B. number of EC2 instances on AWS account exceeded
- C. EBS volume limits exceeded
- D. multiple IP addresses assigned to instance
- E. unsupported instance type assigned

Answer (B,C)



- Question 22: You recently made some configuration changes to an EC2 instance. You then launched a new EC2 instance from the same AMI however none of the settings were saved. What is the cause of this error?
- A. did not save configuration changes to EC2 instance
 - B. did not save configuration changes to AMI
 - C. did not create new AMI
 - D. did not reboot EC2 instance to enable changes

Answer (C)

- Question 23: What statements are correct concerning DisableApiTermination attribute? (Select two)

- A. cannot enable termination protection for Spot instances
- B. termination protection is disabled by default for an EC2 instance
- C. termination protection is enabled by default for an EC2 instance
- D. can enable termination protection for Spot instances
- E. DisableApiTermination attribute supported for EBS-backed instances only

Answer (A,B)

Question 24:

- What is required to copy an encrypted EBS snapshot cross-account? (Select two)

- A. copy the unencrypted EBS snapshot to an S3 bucket
- B. distribute the custom key from CloudFront
- C. share the custom key for the snapshot with the target account
- D. share the encrypted EBS snapshot with the target account
- E. share the encrypted EBS snapshots publicly
- F. enable root access security on both accounts

Answer (C,D)

Question 25:

- What three services enable Single-AZ as a default?

- A. EC2
- B. ELB
- C. Auto-Scaling
- D. DynamoDB
- E. S3

Answer (A,B,C)

Question 26:

- What AWS service automatically publishes access logs every five minutes?

- A. VPC Flow Logs
- B. Elastic Load Balancer
- C. CloudTrail
- D. DNS Route 53

Answer (B)

Question 27:

- You have developed a web-based application for file sharing that will allow customers to access files. There are a variety of sizes that include larger .pdf and video files. What two solution stacks could tenants use for an online file sharing service? (Select two)

- A. EC2, ELB, Auto-Scaling, S3
- B. Route 53, Auto-Scaling, DynamoDB
- C. EC2, Auto-Scaling, RDS
- D. CloudFront

Answer (A,D)

Question 28:

- What infrastructure services are provided to EC2 instances? (Select three)



- A. VPN
- B. storage
- C. compute
- D. transport
- E. security
- F. support

Answer (B,C,D)

Question 29:

What steps are required from AWS console to copy an EBS-backed AMI for a database instance cross-region?

- A. create Snapshot of data volume, select Copy, select destination region
- B. select Copy EBS-backed AMI option and destination region
- C. select copy database volume and destination region
- D. create Snapshot of EBS-backed AMI, select Copy Snapshot option, select destination region
- E. create Snapshot of Instance-store AMI, select Copy AMI option, select destination region

Answer (D)

Question 30:

How is capacity (compute, storage and network speed) managed and assigned to EC2 instances?

- A. AMI
- B. instance type
- C. IOPS
- D. Auto-Scaling

Answer (B)

Question 31:

What storage type enable permanent attachment of volumes to EC2 instances?

- A. S3
- B. RDS
- C. TDS
- D. EBS
- E. instance store

Answer (D)

Question 32: What is the recommended method for migrating (copying) an EC2 instance to a different region?

- A. terminate instance, select region, copy instance to destination region
- B. select AMI associated with EC2 instance and use Copy AMI option
- C. stop instance and copy AMI to destination region
- D. cross-region copy is not currently supported

Answer (B)

Question 33:

What are two attributes that define an EC2 instance type?

- A. vCPU
- B. license type
- C. EBS volume storage
- D. IP address
- E. Auto-Scaling

Answer (A,C)

Question 34:

How is an Amazon Elastic Load Balancer (ELB) assigned?

- A. per EC2 instance
- B. per Auto-Scaling group



C. per subnet

D. per VPC

Answer (A)

Question 35:

What method detects when to replace an EC2 instance that is assigned to an Auto-Scaling group?

A. health check

B. load balancing algorithm

C. EC2 health check

D. not currently supported

E. dynamic path detection

F. Auto-Scaling

Answer (A)

Question 36:

What two statements correctly describe Auto-Scaling groups?

A. horizontal scaling of capacity

B. decrease number of instances only

C. EC2 instances are assigned to a group

D. database instances only

E. no support for multiple availability zones

Answer (A,C)

Question 37:

What is the default maximum number of Elastic IP addresses assignable per Amazon AWS region?

A. 1

B. 100

C. 5

D. unlimited

Answer (C)

Question 38:

How are snapshots for an EBS volume created when it is the root device for an instance?

A. pause instance, unmount volume and snapshot

B. terminate instance and snapshot

C. unencrypt volume and snapshot dynamically

D. stop instance, unmount volume and snapshot

Answer (D)

Question 39:

What cloud compute components are configured by tenants and not Amazon AWS support engineers? (Select three)

A. hypervisor

B. upstream physical switch

C. virtual appliances

D. guest operating system

E. applications and databases

F. RDS

Answer (C,D,E)

Question 40:

What three attributes are used to define a launch configuration template for an Auto-Scaling group?

A. instance type

B. private IP address

C. Elastic IP



D. security group

E. AMI

Answer (A,D,E)

Question 41:

What three characteristics or limitations differentiate EC2 instance types?

A. VPC only

B. application type

C. EBS volume only

D. virtualization type

E. AWS service selected

Answer (A,C,D)

Question 42:

Select two difference between HVM and PV virtualization types?

A. HVM supports all current generation instance types

B. HVM is similar to bare metal hypervisor architecture

C. PV provides better performance than HVM for most instance types

D. HVM doesn't support enhanced networking

E. HVM doesn't support current generation instance types

Answer (A,B)

Virtual Private Cloud (VPC) Question 1: What are the minimum components required to enable a web-based application with public web servers and a private database tier? (select three)

A. Internet gateway

B. Assign EIP addressing to database instances on private subnet

C. Virtual private gateway

D. Assign database instances to private subnet and private IP addressing

E. Assign EIP and private IP addressing to web servers on public subnet

Answer (A,D,E)

Question 2:

Refer to the network drawing. How are packets routed from private subnet to public subnet for the following web-based application with a database tier?

A. Internet gateway

B. custom route table

C. 10.0.0.0/16

D. nat-instance-id

E. igw-id

F. add custom route table

Answer (D)

Question 3:

What VPC component provides Network Address Translation?

A. NAT instance

B. NAT gateway

C. virtual private gateway

D. Internet gateway

E. ECS

Answer (D)

Question 4:

What are the advantages of NAT gateway over NAT instance? (Select two)

A. NAT gateway requires a single EC2 instance

B. NAT gateway is scalable

C. NAT gateway translates faster

D. NAT gateways is a managed service

E. NAT gateway is Linux-based



Answer (B,D)

Question 5:

What is the management responsibility of tenants and not Amazon AWS?

- A. EC2 instances
- B. RDS
- C. Beanstalk
- D. NAT instance

Answer (A,D)

Question 6:

What two features provide an encrypted (VPN) connection from VPC to an enterprise data center?

- A. Internet gateway
- B. Amazon RDS
- C. Virtual private gateway
- D. CSR 1000V router
- E. NAT gateway

Answer (C,D)

Question 7:

What two attributes are supported when configuring an Amazon Virtual private gateway (VPG)?

- A. route propagation
- B. Elastic IP (EIP)
- C. DHCP
- D. public IPv4 address
- E. public subnets

Answer (A,C)

Question 8:

What two features are available with AWS Direct Connect service?

- A. internet access
- B. extend on-premises VLANs to cloud
- C. bidirectional forwarding detection (BFD)
- D. load balancing between Direct Connect and VPN connection
- E. public and private AWS services

Answer (C,E)

Question 9:

When is Direct Connect a preferred solution over VPN IPsec?

- A. fast and reliable connection
- B. redundancy is a key requirement
- C. fast and easy to deploy
- D. layer 3 connectivity
- E. layer 2 connectivity

Answer (A)

Question 10:

You have been asked to setup a VPC endpoint connection between VPC and S3 buckets for storing backups and snapshots. What AWS components are currently required when configuring a VPC endpoint?

- A. Internet gateway
- B. NAT instance
- C. Elastic IP
- D. private IP address

Answer (D)

Question 11:

What are the primary advantages of VPC endpoints? (Select two)



- A. reliability
- B. cost
- C. throughput
- D. security

Answer (B,D)

Question 12:

What are the DHCP option attributes used to assign private DNS servers to your VPC?

- A. dns resolution and domain name
- B. hostnames and internet domain
- C. domain servers and domain name
- D. domain-name-servers and domain-name

Answer (D)

Question 13:

What DNS attributes are configured when Default VPC option is selected?

- A. DNS resolution: yes / DNS hostnames: yes
- B. DNS resolution: yes / DNS hostnames: no
- C. DNS resolution: no / DNS hostnames: yes
- D. DNS resolution: no / DNS hostnames: no

Answer (A)

Question 14:

What configuration settings are required from the remote VPC in order to create cross-account peering? (Select three)

- A. VPC ID
- B. account username
- C. account ID
- D. CMK keys
- E. VPC CIDR block
- F. volume type

Answer (A,C,E)

Question 15:

What CIDR block range is supported for IPv4 addressing and subnetting within a single VPC?

- A. /16 to /32
- B. /16 to /24
- C. /16 to /28
- D. /16 to /20

Answer (C)

Question 16: What problem is caused by the fact that VPC peering does not permit transitive routing?

- A. additional VPC route tables to manage
- B. virtual private gateway is required
- C. Internet gateway is required for each VPC
- D. routing between connected spokes through hub VPC is complex
- E. increased number of peer links required

Answer (E)

Question 17:

What two statements correctly describes Elastic Load Balancer operation?

- A. spans multiple regions
- B. assigned per EC2 instance
- C. assigned per subnet
- D. assigned per Auto-Scaling group
- E. no cross-region support



Answer (D,E)

Question 18:

What are two advantages of Elastic IP (EIP) over AWS public IPv4 addresses?

- A. EIP can be reassigned
- B. EIP is private
- C. EIP is dynamic
- D. EIP is persistent
- E. EIP is public and private

Answer (A,D)

Question 19:

What AWS services are globally managed? (Select four)

- A. IAM
- B. S3
- C. CloudFront
- D. Route 53
- E. DynamoDB
- F. WAF
- G. ELB

Answer (A,C,D,F)

Question 20:

What methods are available for creating a VPC? (Select three)

- A. AWS management console
- B. AWS marketplace
- C. VPC wizard
- D. VPC console
- E. Direct Connect

Answer (A,C,D)

Question 21: What two default settings are configured for tenants by AWS

when Default VPC option is selected?

- A. creates a size /20 default subnet in each Availability Zone
- B. creates an Internet gateway
- C. creates a main route table with local route 10.0.0.0/16
- D. create a virtual private gateway
- E. create a security group that explicitly denies all traffic

Answer (A,B)

Question 22:

What three statements correctly describes IP address allocation within a VPC?

- A. EC2 instance must be terminated to reassign an IP address
- B. EC2 instance that is paused can reassign IP address
- C. EC2 instance that is stopped can reassign IP address
- D. private IP addresses are allocated from a pool and can be reassigned
- E. private IP addresses can be assigned by tenant
- F. VPC supports dual stack mode (IPv4/IPv6)

Answer (A,E,F)

Question 23:

What are two advantages of selecting default tenancy option for your VPC when creating it?

- A. performance and reliability
- B. some AWS services do not work with a dedicated tenancy VPC
- C. tenant can launch instances within VPC as default or dedicated instances
- D. instance launch is faster

Answer (B,C)

Question 24: What is the purpose of a local route within a VPC route table?



- A. local route is derived from the default VPC CIDR block 10.0.0.0/16
- B. communicate between instances within the same subnet or different subnets
- C. used to communicate between instances within the same subnet
- D. default route for communicating between private and public subnets
- E. only installed in the main route table

Answer (C)

Question 25:

What is the default behavior when adding a new subnet to your VPC? (Select two)

- A. new subnet is associated with the main route table
- B. new subnet is associated with the custom route table
- C. new subnet is associated with any selected route table
- D. new subnet is assigned to the default subnet
- E. new subnet is assigned from the VPC CIDR block

Answer (A,E)

Question 26: You have enabled Amazon RDS database services in VPC1 for an application that has public web servers in VPC2. How do you connect the web servers to the RDS database instance so they can communicate considering the VPC's are in the same region?

- A. VPC endpoints
- B. VPN gateway
- C. path-based routing
- D. VPC peering
- E. AWS Network Load Balancer

Answer (D)

Question 27:

What AWS services now support VPC endpoints feature for optimizing security?

(Select three)

- A. Kinesis
- B. DNS Route 53
- C. S3
- D. DynamoDB
- E. RDS

Answer (A,C,D)

Question 28:

What are three characteristics of an Amazon Virtual Private Cloud?

- A. public and private IP addressing
- B. broadcasts
- C. multiple private IP addresses per network interface
- D. dedicated single tenant hardware only
- E. persistent public IP addresses
- F. HSRP

Answer (A,C,E)

Question 29: What is the difference between VPC main route table and custom route table?

- A. VPC only creates a main route table when started
- B. custom route table is the default
- C. custom route table is created for public subnets
- D. custom route table is created for private subnets
- E. main route table is created for public and private subnets

Answer (C)

Question 30:



What is the purpose of the native VPC router?

- A. route packets across the internet
- B. route packets between private cloud instances
- C. route packets between subnets
- D. route packets from instances to S3 storage volumes
- E. route packets across VPN

Answer (C)

Question 31:

How are private DNS servers assigned to an Amazon VPC?

- A. not supported
- B. select nondefault VPC
- C. select default VPC
- D. select EC-2 classic

Answer (B)

Question 32:

What are two characteristics of an Amazon security group?

- A. instance level packet filtering
- B. deny rules only
- C. permit rules only
- D. subnet level packet filtering
- E. inbound only

Answer (A,C)

Question 33:

What statement is true of Network Access Control Lists (ACL) operation within an Amazon VPC?

- A. instance and subnet level packet filtering
- B. subnet level packet filtering
- C. inbound only
- D. only one ACL allowed per VPC
- E. outbound only

Answer (B)

Question 34:

How are packets forwarded between public and private subnets within VPC?

- A. EIP
- B. NAT
- C. main route table
- D. VPN

Answer (B)

Question 35:

What two statements accurately describe Amazon VPC architecture?

- A. Elastic Load Balancer (ELB) cannot span multiple availability zones
- B. VPC does not support DMVPN connection
- C. VPC subnet cannot span multiple availability zones
- D. VPC cannot span multiple regions
- E. Flow logs are not supported within a VPC

Answer (C,D)

Question 36:

What is a requirement for attaching EC2 instances to on-premises clients and applications?

- A. Amazon Virtual Private Gateway (VPN)
- B. Amazon Internet Gateway
- C. VPN Connection
- D. Elastic Load Balancer (ELB)



E. NAT**Answer (B)****Question 37:**

What two statements correctly describe Amazon virtual private gateway?

- A. assign to private subnets only
- B. assign to public subnets only
- C. single virtual private gateway per VPC
- D. multiple virtual private gateways per VPC
- E. single virtual private gateway per region

Answer (A,C)**Question 38:**

What is the maximum access port speed available with Amazon Direct Connect service?

- A. 1 Gbps
- B. 10 Gbps
- C. 500 Mbps
- D. 100 Gbps
- E. 100 Mbps

Answer (B)**Question 39:**

Refer to the drawing. Your company has asked you to configure a peering link between two VPCs that are currently not connected or exchanging any packets.

What destination and target is configured in the routing table of VPC1 to enable packet forwarding to VPC2?

- A. destination = 172.16.0.0/16
target = pcx-vpc2vpc1
- B. destination = 10.0.0.0/16
target = pcx-vpc2
- C. destination = 172.16.0.0/16
target = 10.0.0.0/16
- D. destination = 172.16.0.0/16
target = pcx-vpc1vpc2
- E. default route only

Answer (D)**Question 40:**

How is routing enabled by default within a VPC for an EC2 instance?

- A. add a default route
- B. main route table
- C. custom route table
- D. must be configured explicitly

Answer (B)**Question 41:**

What three features are not supported with VPC peering?

- A. overlapping CIDR blocks
- B. IPv6 addressing
- C. Gateways
- D. transitive routing
- E. RedShift
- F. ElastiCache

Answer (A,C,D)**Question 42:**

What route is used in a VPC routing table for packet forwarding to a Gateway?

- A. static route



- B. 10.0.0.0/16
- C. tenant configured
- D. 0.0.0.0/0
- E. 0.0.0.0/16

Answer (D)

Question 43: You are asked to deploy a web application comprised of multiple public web servers with only private addressing assigned. What Amazon AWS solutions enables multiple servers on a private subnet with only a single EIP required and Availability Zone redundancy?

- A. NAT instance
- B. Internet gateway
- C. virtual private gateway
- D. NAT gateway
- E. Elastic Network Interface (ENI)

Answer (D)

Question 44:

What is the IP addressing schema assigned to a default VPC?

- A. 172.31.0.0/16 CIDR block subnetted with 172.31.0.0/20
- B. 172.16.0.0/16 CIDR block subnetted with 172.16.0.0/24
- C. 10.0.0.0/16 CIDR block subnetted with 10.0.0.0/24
- D. 172.16.0.0/24 CIDR block subnetted with 172.31.0.0/18

Answer (A)

Question 45:

What default configuration and components are added by AWS when Default VPC type is selected? (Select three)

- A. Internet gateway
- B. virtual private gateway
- C. NAT instance
- D. security group
- E. DNS

Answer (A,D,E)

Question 46:

What feature requires tenants to disable source/destination check?

- A. Elastic IP (EIP)
- B. data replication
- C. VPC peering
- D. NAT
- E. Internet gateway

Answer (D)

Storage Services

Question 1:

What AWS storage solution allows thousands of EC2 instances to simultaneously upload, access, delete and share files?

- A. EBS
- B. S3
- C. Glacier
- D. EFS

Answer (D)

Question 2:

What is required for an EFS mount target? (Select two)

- A. EIP
- B. DNS name
- C. IP address



D. DHCP

E. IAM role

Answer (B,C)

Question 3:

What connectivity features are recommended for copying on-premises files to EFS? (Select two)

A. VPN IPsec

B. Internet Gateway

C. Direct Connect

D. File Sync

E. FTP

F. AWS Storage Gateway

Answer (C,D)

Question 4:

What AWS services encrypts data at rest by default? (Select two)

A. S3

B. AWS Storage Gateway

C. EBS

D. Glacier

E. RDS

Answer (B,D)

Question 5:

What fault tolerant features does S3 storage provide? (Select three)

A. cross-region replication

B. versioning must be disabled

C. cross-region asynchronous replication of objects

D. synchronous replication of objects within a region

E. multiple destination buckets

Answer (A,C,D)

Question 6:

What is the fastest technique for deleting 900 objects in an S3 bucket with a single HTTP request?

A. Multi-Part Delete API

B. Multi-Object Delete API

C. 100 objects is maximum per request

D. Fast-Delete API

Answer (B)

Question 7:

What security controls technique is recommended for S3 cross-account access?

A. IAM group

B. security groups

C. S3 ACL

D. bucket policies

Answer (D)

Question 8:

What are two advantages of cross-region replication of an S3 bucket?

A. cost

B. security compliance

C. scalability

D. Beanstalk support

E. minimize latency

Answer (B,E)

Question 9:



What are two primary difference between Amazon S3 Standard and S3/RRS storage classes?

- A. Amazon Standard does not replicate at all
- B. RRS provides higher durability
- C. RRS provides higher availability
- D. RRS does not replicate objects as many times
- E. application usage is different

Answer (D,E)

Question 10:

What two features are enabled with S3 services?

- A. store objects of any size
- B. dynamic web content
- C. supports Provisioned IOPS
- D. store virtually unlimited amounts of data
- E. bucket names are globally unique

Answer (D,E)

Question 11:

What new feature was recently added to SQS that defines how messages are ordered?

- A. streams
- B. SNS
- C. FIFO
- D. TLS
- E. decoupling

Answer (C)

Question 12:

What two AWS storage types are persistent?

- A. ephemeral
- B. S3
- C. EBS
- D. instance store
- E. SAML

Answer (B,C)

Question 13:

Select three on-premises backup solutions used for copying data to an Amazon AWS S3 bucket?

- A. AWS Import/Export
- B. RDS
- C. Snowball
- D. Availability Zone (AZ) replication
- E. AWS Storage Gateway

Answer (A,C,E)

Question 14:

You have 1 TB of data and want to archive the data that won't be accessed that often. What Amazon AWS storage solution is recommended?

- A. Glacier
- B. EBS
- C. ephemeral
- D. CloudFront

Answer (A)

Question 15:

What are three methods of accessing DynamoDB for customization purposes?

- A. CLI



B. AWS console

C. API call

D. vCenter

E. Beanstalk

Answer (A,B,C)

Question 16:

What are two primary differences between Glacier and S3 storage services?

A. Glacier is lower cost

B. S3 is lower cost

C. Glacier is preferred for frequent data access with lower latency

D. S3 is preferred for frequent data access with lower latency

E. S3 supports larger file size

Answer (A,D)

Question 17:

What statement correctly describes the operation of AWS Glacier archive?

A. archive is a group of vaults

B. archive is an unencrypted vault

C. archive supports aggregated files only

D. maximum file size is 1 TB

E. archive supports single and aggregated files

Answer (E)

Question 18: What are three primary differences between S3 vs EBS?

A. S3 is a multi-purpose public internet-based storage

B. EBS is directly assigned to a tenant VPC EC2 instance

C. EBS and S3 provide persistent storage

D. EBS snapshots are typically stored on S3 buckets

E. EBS and S3 use buckets to manage files

F. EBS and S3 are based on block level storage

Answer (A,B,D)

Question 19:

What on-premises solution is available from Amazon AWS to minimize latency

for all data?

A. Gateway-VTL

B. Gateway-cached volumes

C. Gateway-stored volumes

D. EBS

E. S3 bucket

F. ElastiCache

Answer (C)

Question 20:

What feature transitions S3 storage to Standard-IA for cost optimization?

A. RRS/S3

B. Glacier vault

C. storage class analysis

D. path-based routing

Answer (C)

Question 21:

How does AWS uniquely identify S3 objects?

A. bucket name

B. version

C. key

D. object tag

Answer (C)



Question 22:

What is the advantage of read-after-write consistency for S3 buckets?

- A. no stale reads for PUT of any new object in all regions
- B. higher throughput for all requests
- C. stale reads for PUT requests in some regions
- D. no stale reads for GET requests in a single regions

Answer (A)

Question 23:

What is the maximum single file object size supported with Amazon S3?

- A. 5 GB
- B. 5 TB
- C. 1 TB
- D. 100 GB

Answer (B)

Question 24:

What security problem is solved by using Cross-Origin Resource Sharing (CORS)?

- A. enable HTTP requests from within scripts to a different domain
- B. enable sharing of web-based files between different buckets
- C. provide security for third party objects within AWS
- D. permits sharing objects between AWS services

Answer (A)

Question 25:

What is recommended for migrating 40 TB of data from on-premises to S3 when the internet link is often overutilized?

- A. AWS Storage gateway
- B. AWS Snowball
- C. AWS Import/Export
- D. AWS Elastic File System
- E. AWS Elasticsearch
- F. AWS Multi-Part Upload API

Answer (B)

Question 26:

Your company is publishing an online catalog of books that is currently using DynamoDB for storing the information associated with each item. There is a requirement to add images for each book. What solution is most cost effective and designed for that purpose?

- A. RedShift
- B. EBS
- C. RDS
- D. S3
- E. Kinesis

Answer (D)

Question 27:

You have an application that collects monitoring data from 10,000 sensors (IoT) deployed in the USA. The datapoints are comprised of video events for home security and environment status alerts. The application will be deployed to AWS with EC2 instances as data collectors. What AWS storage service is preferred for storing video files from sensors?

- A. RedShift
- B. RDS
- C. S3
- D. DynamoDB



Answer (C)**Security Architecture****Question 1:**

What statements correctly describe security groups within a VPC? (Select three)

- A. default security group only permit inbound traffic
- B. security groups are stateful firewalls
- C. only allow rules are supported
- D. allow and deny rules are supported
- E. security groups are associated to network interfaces

Answer (B,C,E)

Question 2:

What three items are required to configure a security group rule?

- A. protocol type
- B. VPC name
- C. port number
- D. source IP
- E. destination IP
- F. description

Answer (A,C,D)

Question 3:

What two source IP address types are permitted in a security group rule?

- A. only CIDR blocks with /16 subnet mask
- B. source IP address 0.0.0.0/0
- C. single source IP address with /24 subnet mask
- D. security group id
- E. IPv6 address with /64 prefix length

Answer (B,D)

Question 4:

What protocols must be enabled for remote access to Linux-based and Windowsbased EC2 instances?

- A. SSH, ICMP, Telnet
- B. SSH, HTTP, RDP
- C. SSH, HTTP, SSL
- D. SSH, RDP, ICMP

Answer (D)

Question 5:

Distinguish network ACLs from security groups within a VPC? (Select three)

- A. ACL filters at the subnet level
- B. ACL is based on deny rules only
- C. ACL is applied to instances and subnets
- D. ACL is stateless
- E. ACL supports a numbered list for filtering

Answer (A,D,E)

Question 6:

What happens to the security permissions of a tenant when an IAM role is granted? (Select two)

- A. tenant inherits only permissions assigned to the IAM role temporarily
- B. add security permissions of the IAM role to existing permissions
- C. previous security permissions are no longer in effect
- D. previous security permissions are deleted unless reconfigured
- E. tenant inherits only read permissions assigned to the IAM role

Answer (A,C)

Question 7:

Where are IAM permissions granted to invoke and execute a Lambda function



for S3 access? (Select two)

- A. S3 bucket
- B. EC2 instance
- C. Lambda function
- D. IAM role
- E. event mapping

Answer (A,D)

Question 8:

You have some developers working on code for an application and they require temporary access to AWS cloud up to an hour. What is the easiest web-based solution from AWS to provide access and minimize security exposure?

- A. ACL
- B. security group
- C. IAM group
- D. STS
- E. EFS

Answer (D)

Question 9:

What two methods are used to request temporary credentials based on AWS Security Token Service (STS)?

- A. Web Identity Federation
- B. LDAP
- C. IAM identity
- D. dynamic ACL
- E. private key rotation

Answer (A,C)

Question 10:

What two components are required for enabling SAML authentication requests to AWS Identity and Access Management (IAM)?

- A. access keys
- B. session token
- C. SSO
- D. identity provider (IdP)
- E. SAML provider entity

Answer (D,E)

Question 11:

What are two reasons for deploying Origin Access Identity (OAI) when enabling CloudFront?

- A. prevent users from deleting objects in S3 buckets
- B. mitigate distributed denial of service attacks (DDoS)
- C. prevent users from accessing objects with Amazon S3 URL
- D. prevent users from accessing objects with CloudFront URL
- E. replace IAM for internet-based customer authentication

Answer (B,C)

Question 12:

What solutions are recommended to mitigate DDoS attacks? (Select three)

- A. host-based firewall
- B. elastic load balancer
- C. WAF
- D. SSL/TLS
- E. Bastion host
- F. NAT gateway

Answer (B,C,E)



Question 13:

What features are required to prevent users from bypassing AWS CloudFront security? (Select three)

- A. Bastion host
- B. signed URL
- C. IP whitelist
- D. signed cookies
- E. origin access identity (OAI)

Answer (B,D,E)

Question 14:

What is the advantage of resource-based policies for cross-account access?

- A. trusted account permissions are not replaced
- B. trusted account permissions are replaced
- C. resource-based policies are easier to deploy
- D. trusting account manages all permissions

Answer (A)

Question 15:

Select three requirements for configuring a Bastion host?

- A. EIP
- B. SSH inbound permission
- C. default route
- D. CloudWatch logs group
- E. VPN
- F. Auto-Scaling

Answer (A,B,D)

Question 16:

What rule must be added to the security group assigned to a mount target instance that enables EFS access from an EC2 instance?

- A. Type = EC2, protocol = IP, port = 2049, source = remote security group id
- B. Type = EC2, protocol = EFS, port = 2049, source = 0.0.0.0/0
- C. Type = NFS, protocol = TCP, port = 2049, source = remote security group id
- D. Type = NFSv4, protocol = UDP, port = 2049, source = remote security group id

Answer (C)

Question 17: What statement correctly describes IAM architecture?

- A. IAM security is unified per region and replicated based on requirements for an AWS tenant account
- B. IAM security is defined per region for roles only on an AWS tenant account
- C. IAM security is globally unified across the AWS cloud for an AWS tenant account
- D. IAM security is defined separately per region and cross-region security enabled for an AWS tenant account

Answer (C)

Question 18:

What are two advantages of customer-managed encryption keys (CMK)?

- A. create and rotate encryption keys
- B. AES-128 cipher for data at rest
- C. audit encryption keys
- D. encrypts data in-transit for server-side encryption only

Answer (A,C)



Question 19:

What feature is not available with AWS Trusted Advisor?

- A. cost optimization
- B. infrastructure best practices
- C. vulnerability assessment
- D. monitor application metrics

Answer (C)

Question 20:

What is required to Ping from a source instance to a destination instance?

- A. Network ACL: not required Security Group: allow ICMP outbound on source/destination EC2 instances
- B. Network ACL: allow ICMP inbound/outbound on source/destination subnets Security Group: not required
- C. Network ACL: allow ICMP inbound/outbound on source/destination subnets Security Group: allow ICMP outbound on source EC2 instance Security Group: allow ICMP inbound on destination EC2 instance
- D. Network ACL: allow TCP inbound/outbound on source/destination subnets Security Group: allow TCP and ICMP inbound on source EC2 instance

Answer (C)

Question 21:

What two steps are required to grant cross-account permissions between AWS accounts?

- A. create an IAM user
- B. attach a trust policy to S3
- C. create a transitive policy
- D. attach a trust policy to the role
- E. create an IAM role

Answer (D,E)

Question 22: You have configured a security group to allow ICMP, SSH and RDP inbound and assigned the security group to all instances in a subnet. There is no access to any Linux-based or Windows-based instances and you cannot Ping any instances. The network ACL for the subnet is configured to allow all inbound traffic to the subnet. What is the most probable cause?

- A. on-premises firewall rules
- B. security group and network ACL outbound rules
- C. network ACL outbound rules
- D. security group outbound rules
- E. Bastion host required

Answer (C)

Question 23:

What three techniques provide authentication security on S3 volumes?

- A. bucket policies
- B. network ACL
- C. Identity and Access Management (IAM)
- D. encryption
- E. AES256

Answer (A,B,C)

Question 24: What statement correctly describes support for AWS encryption of S3 objects?

- A. tenants manage encryption for server-side encryption of S3 objects
- B. Amazon manages encryption for server-side encryption of S3 objects
- C. client-side encryption of S3 objects is not supported
- D. S3 buckets are encrypted only



E. SSL is only supported with Glacier storage

Answer (B)

Question 25:

What authentication method provides Federated Single Sign-On (SSO) for cloud applications?

- A. ADS
- B. ISE
- C. RADIUS
- D. TACACS
- E. SAML

Answer (E)

Question 26:

Based on the Amazon security model, what infrastructure configuration and associated security is the responsibility of tenants and not Amazon AWS? (Select two)

- A. dedicated cloud server
- B. hypervisor
- C. operating system level
- D. application level
- E. upstream physical switch

Answer (C,D)

Question 27:

What security authentication is required before configuring or modifying EC2 instances? (Select three)

- A. authentication at the operating system level
- B. EC2 instance authentication with asymmetric keys
- C. authentication at the application level
- D. Telnet username and password
- E. SSH/RDP session connection

Answer (A,B,E)

Question 28:

What feature is part of Amazon Trusted Advisor?

- A. security compliance
- B. troubleshooting tool
- C. EC2 configuration tool
- D. security certificates

Answer (A)

Question 29:

What are two best practices for account management within Amazon AWS?

- A. do not use root account for common administrative tasks
- B. create a single AWS account with multiple IAM users that have root privilege
- C. create multiple AWS accounts with multiple IAM users per AWS account
- D. use root account for all administrative tasks
- E. create multiple root user accounts for redundancy

Answer (A,C)

Question 30:

What AWS feature is recommended for optimizing data security?

- A. Multi-factor authentication
- B. username and encrypted password
- C. Two-factor authentication
- D. SAML



E. Federated LDAP**Answer (A)****Question 31:**

What IAM class enables an EC2 instance to access a file object in an S3 bucket?

- A. user
- B. root
- C. role
- D. group

Answer (C)**Question 32:**

What are three recommended solutions that provide protection and mitigation from distributed denial of service (DDoS) attacks?

- A. security groups
- B. CloudWatch
- C. encryption
- D. WAF
- E. data replication
- F. Auto-Scaling

Answer (A,B,D)**Question 33:**

What are three recommended best practices when configuring Identity and Access Management (IAM) security services?

- A. Lock or delete your root access keys when not required
- B. IAM groups are not recommended for storage security
- C. create an IAM user with administrator privileges
- D. share your password and/or access keys with members of your group only
- E. delete any AWS account where the access keys are unknown

Answer (A,C,E)**Question 34:**

What two features create security zones between EC2 instances within a VPC?

- A. security groups
- B. Virtual Security Gateway
- C. network ACL
- D. WAF

Answer (A,B)**Question 35:**

What AWS service provides vulnerability assessment services to tenants within the cloud?

- A. Amazon WAF
- B. Amazon Inspector
- C. Amazon Cloud Logic
- D. Amazon Trusted Advisor

Answer (B)**Question 36:**

What are two primary differences between AD Connector and Simple AD for cloud directory services?

- A. Simple AD requires an on-premises ADS directory
- B. Simple AD is fully managed and setup in minutes
- C. AD Connector requires an on-premises ADS directory
- D. Simple AD is more scalable than AD Connector
- E. Simple AD provides enhanced integration with IAM

Answer (B,C)

Database Services**Question 1:**

How is load balancing enabled for multiple tasks to the same container instance?

- A. path-based routing
- B. reverse proxy
- C. NAT
- D. dynamic port mapping
- E. dynamic listeners

Answer (D)

Question 2:

What encryption support is available for tenants that are deploying AWS DynamoDB?

- A. server-side encryption
- B. client-side encryption
- C. client-side and server-side encryption
- D. encryption not supported
- E. block level encryption

Answer (B)

Question 3:

What are three primary reasons for deploying ElastiCache?

- A. data security
- B. managed service
- C. replication with Redis
- D. durability
- E. low latency

Answer (B,C,E)

Question 4:

What service does not support session data persistence store to enable web-based stateful applications?

- A. RDS
- B. Memcached
- C. DynamoDB
- D. Redis
- E. RedShift

Answer (B)

Question 5:

How does Memcached implement horizontal scaling?

- A. Auto-Scaling
- B. database store
- C. partitioning
- D. EC2 instances
- E. S3 bucket

Answer (C)

Question 6:

What two options are available for tenants to access ElastiCache?

- A. VPC peering link
- B. EC2 instances
- C. EFS mount
- D. cross-region VPC

Answer (A,B)

Question 7:

What two statements correctly describe in-transit encryption support on ElastiCache platform ?



- A. not supported for ElastiCache platform
- B. supported on Redis replication group
- C. encrypts cached data at rest
- D. not supported on Memcached cluster
- E. IPsec must be enabled first

Answer (B,D)

Question 8:

What Amazon AWS platform is designed for complex analytics of a variety of large data sets based on custom code. The applications include machine learning and data transformation?

- A. EC2
- B. Beanstalk
- C. Redshift
- D. EMR

Answer (D)

Question 9:

What are two primary advantages of DynamoDB?

- A. SQL support
- B. managed service
- C. performance
- D. CloudFront integration

Answer (B,C)

Question 10:

What two fault tolerant features does Amazon RDS support?

- A. copy snapshot to a different region
- B. create read replica to a different region
- C. copy unencrypted read-replica only
- D. copy read/write replica and snapshot

Answer (A,B)

Question 11:

What managed services are included with Amazon RDS? (select four)

- A. assign network capacity to database instances
- B. install database software
- C. perform regular backups
- D. data replication across multiple availability zones
- E. data replication across single availability zone only
- F. configure database
- G. performance tuning

Answer (A,B,C,D)

Question 12:

What two configuration features are required to create a private database instance?

- A. security group
- B. network ACL
- C. CloudWatch
- D. Elastic IP (EIP)
- E. Nondefault VPC
- F. DNS

Answer (A,F)

Question 13:

What storage type is recommended for an online transaction processing (OLTP) application deployed to Multi-AZ RDS with significant workloads?

- A. General Purpose SSD



- B. Magnetic
- C. EBS volumes
- D. Provisioned IOPS

Answer (D)

Question 14:

What features are supported with Amazon RDS? (Select three)

- A. horizontal scaling with multiple read replicas
- B. elastic load balancing RDS read replicas
- C. replicate read replicas cross-region
- D. automatic failover to master database instance
- E. application load balancer (ALB)

Answer (A,C,E)

Question 15:

What are three advantages of standby replica in a Multi-AZ RDS deployment?

- A. fault tolerance
- B. eliminate I/O freezes
- C. horizontal scaling
- D. vertical scaling
- E. data redundancy

Answer (A,B,E)

Question 16:

What consistency model is the default used by DynamoDB?

- A. strongly consistent
- B. eventually consistent
- C. no default model
- D. casual consistency
- E. sequential consistency

Answer (B)

Question 17:

What does RDS use for database and log storage?

- A. EBS
- B. S3
- C. instance store
- D. local store
- E. SSD

Answer (A)

Question 18:

What statements correctly describe support for Microsoft SQL Server within Amazon VPC? (Select three)

- A. read/write replica
- B. read replica only
- C. vertical scaling
- D. native load balancing
- E. EBS storage only
- F. S3 storage only

Answer (B,C,D)

Question 19:

Select two features available with Amazon RDS for MySQL?

- A. Auto-Scaling
- B. read requests to standby replicas
- C. real-time database replication
- D. active read requests only

Answer (B,C)



Question 20:

What are two characteristics of Amazon RDS?

- A. database managed service
- B. NoSQL queries
- C. native load balancer
- D. database write replicas
- E. automatic failover of read replica

Answer (A,C)

Question 21:

What caching engines are supported with Amazon ElastiCache? (Select two)

- A. HAProxy
- B. Route 53
- C. RedShift
- D. Redis
- E. Memcached
- F. CloudFront

Answer (D,E)

Question 22:

What are three primary characteristics of DynamoDB?

- A. less scalable than RDS
- B. static content
- C. store metadata for S3 objects
- D. replication to three Availability Zones
- E. high read/write throughput

Answer (C,D,E)

Question 23:

What are three examples of using Lambda functions to move data between AWS services?

- A. read data directly from DynamoDB streams to RDS
- B. read data from Kinesis stream and write data to DynamoDB
- C. read data from DynamoDB stream to Firehose and write to S3
- D. read data from S3 and write metadata to DynamoDB
- E. read data from Kinesis Firehose to Kinesis data stream

Answer (B,C,D)

Question 24: You have enabled Amazon RDS database services in VPC1 for an application with public web servers in VPC2. How do you connect the web servers to the RDS database instance so they can communicate considering the VPC's are in different regions?

- A. VPC endpoints
- B. VPN gateway
- C. path-based routing
- D. publicly accessible database
- E. VPC peering

Answer (D)

Question 25:

You have a requirement to create an index to search customer objects stored in S3 buckets. The solution should enable you to create a metadata search index for each object stored to an S3 bucket. Select the most scalable and cost effective solution?

- A. RDS, ElastiCache
- B. DynamoDB, Lambda
- C. RDS, EMR, ALB
- D. RedShift



Answer (B)

Question 26: What are three advantages of using DynamoDB over S3 for storing IoT sensor data where there are 100,000 datapoint samples sent per minute?

- A. S3 must create a single file for each event
- B. IoT can write data directly to DynamoDB
- C. DynamoDB provides fast read/writes to a structured table for queries
- D. DynamoDB is designed for frequent access and fast lookup of small records
- E. S3 is designed for frequent access and fast lookup of smaller records
- F. IoT can write data directly to S3

Answer (B,C,D)

Question 27:

Your company is a provider of online gaming that customers access with various network access devices including mobile phones. What is a data warehousing solutions for large amounts of information on player behavior, statistics and events for analysis using SQL tools?

- A. RedShift
- B. DynamoDB
- C. RDS
- D. DynamoDB
- E. Elasticsearch

Answer (A)

Question 28: What two statements are correct when comparing Elasticsearch and RedShift as analytical tools?

- A. Elasticsearch is a text search engine and document indexing tool
- B. RedShift supports complex SQL-based queries with Petabyte sized data store
- C. Elasticsearch supports SQL queries
- D. RedShift provides only basic analytical services
- E. Elasticsearch does not support JSON data type

Answer (A,B)

Question 29:

What happens when read or write requests exceed capacity units (throughput capacity) for a DynamoDB table or index? (Select two)

- A. DynamoDB automatically increases read/write units
- B. DynamoDB can throttle requests so that requests are not exceeded
- C. HTTP 400 code is returned (Bad Request)
- D. HTTP 500 code is returned (Server Error)
- E. DynamoDB automatically increases read/write units if provisioned throughput is enabled

Answer (B,C)

Question 30:

What read consistency method provides lower latency for GetItem requests?

- A. strongly persistent
- B. eventually consistent
- C. strongly consistent
- D. write consistent

Answer (B)

Question 31:

You must specify strongly consistent read and write capacity for your DynamoDB database. You have determined read capacity of 128 Kbps and write capacity of 25 Kbps is required for your application. What is the read and write



capacity units required for DynamoDB table?

- A. 32 read units, 25 write units
- B. 1 read unit, 1 write unit
- C. 16 read units, 2.5 write units
- D. 64 read units, 10 write units

Answer (A)

Question 32:

What DynamoDB capacity management technique is based on the tenant specifying an upper and lower range for read/write capacity units?

- A. demand
- B. provisioned throughput
- C. reserved capacity
- D. auto scaling
- E. general purpose

Answer (D)

Question 33:

What is the maximum volume size of a MySQL RDS database?

- A. 6 TB
- B. 3 TB
- C. 16 TB
- D. unlimited

Answer (C)

Question 34:

What is the maximum size of a DynamoDB record (item)?

- A. 400 KB
- B. 64 KB
- C. 1 KB
- D. 10 KB

Answer (A)

Fault Tolerant Systems

Question 1:

What two features describe an Application Load Balancer (ALB)?

- A. dynamic port mapping
- B. SSL listener
- C. layer 7 load balancer
- D. backend server authentication
- E. multi-region forwarding

Answer (A,C)

Question 2:

What enables load balancing between multiple applications per load balancer?

- A. listeners
- B. sticky sessions
- C. path-based routing
- D. backend server authentication

Answer (C)

Question 3:

What three features are characteristic of Classic Load Balancer?

- A. dynamic port mapping
- B. path-based routing
- C. SSL listener
- D. backend server authentication
- E. ECS
- F. Layer 4 based load balancer



Answer (C,D,F)

Question 4:

What security feature is only available with Classic Load Balancer?

- A. IAM role
- B. SAML
- C. back-end server authentication
- D. security groups
- E. LDAP

Answer (C)

Question 5:

What is a primary difference between Classic and Network Load Balancer?

- A. IP address target
- B. Auto-Scaling
- C. protocol target
- D. cross-zone load balancing
- E. listener

Answer (A)

Question 6: What are the first two conditions used by Amazon AWS default termination policy for Multi-AZ architecture?

- A. unprotected instance with oldest launch configuration
- B. Availability Zone (AZ) with the most instances
- C. at least one instance that is not protected from scale in
- D. unprotected instance closest to the next billing hour
- E. random selection of any unprotected instance

Answer (B,C)

Question 7:

What feature is used for horizontal scaling of consumers to process data records from a Kinesis data stream?

- A. vertical scaling shards
- B. Auto-Scaling
- C. Lambda
- D. Elastic Load Balancer

Answer (B)

Question 8:

What DNS records can be used for pointing a zone apex to an Elastic Load Balancer or CloudFront distribution? (Select two)

- A. Alias
- B. CNAME
- C. MX
- D. A
- E. Name Server

Answer (A,D)

Question 9: What services are primarily provided by DNS Route 53? (Select three)

- A. load balancing web servers within a private subnet
- B. resolve hostnames and IP addresses
- C. load balancing web servers within a public subnet
- D. load balancing data replication requests between ECS containers
- E. resolve queries and route internet traffic to AWS resources
- F. automated health checks to EC2 instances

Answer (B,E,F)

Question 10:

What are two features that correctly describe Availability Zone (AZ)



architecture?

- A. multiple regions per AZ
- B. interconnected with private WAN links
- C. multiple AZ per region
- D. interconnected with public WAN links
- E. data auto-replicated between zones in different regions
- F. Direct Connect supports Layer 2 connectivity to region

Answer (B,C)

Question 11:

How is Route 53 configured for Warm Standby fault tolerance? (Select two)

- A. automated health checks
- B. path-based routing
- C. failover records
- D. Alias records

Answer (A,C)

Question 12:

How is DNS Route 53 configured for Multi-Site fault tolerance? (Select two)

- A. IP address
- B. weighted records (non-zero)
- C. health checks
- D. Alias records
- E. zero weighted records

Answer (B,C)

Question 13:

What is an Availability Zone?

- A. data center
- B. multiple VPCs
- C. multiple regions
- D. single region
- E. multiple EC2 server instances

Answer (A)

Question 14:

How are DNS records managed with Amazon AWS to enable high availability?

- A. Auto-Scaling
- B. server health checks
- C. reverse proxy
- D. elastic load balancing

Answer (C)

Question 15:

What is the difference between Warm Standby and Multi-Site fault tolerance?

(Select two)

- A. Multi-Site enables lower RTO and most recent RPO
- B. Warm Standby enables lower RTO and most recent RPO
- C. Multi-Site provides active/active load balancing
- D. Multi-Site provides active/standby load balancing
- E. DNS Route 53 is not required for Warm Standby

Answer (A,C)

Question 16:

What AWS best practice is recommended for creating fault tolerant systems?

- A. vertical scaling
- B. Elastic IP (EIP)
- C. security groups
- D. horizontal scaling



E. RedShift**Answer (D)****Question 17:**

What two statements correctly describe versioning for protecting data at rest on S3 buckets?

- A. enabled by default
- B. overwrites most current file version
- C. restores deleted files
- D. saves multiple versions of a single file
- E. disabled by default

Answer (C,E)**Question 18:**

What two methods are recommended by AWS for protecting EBS data at rest?

- A. replication
- B. snapshots
- C. encryption
- D. VPN

Answer (B,C)

Question 19: You have an Elastic Load Balancer assigned to a VPC with public and private subnets. ELB is configured to load balance traffic to a group of EC2 instances assigned to an Auto-Scaling group. What three statements are correct?

- A. Elastic Load Balancer is assigned to a public subnet
- B. network ACL is assigned to Elastic Load Balancer
- C. security group is assigned to Elastic Load Balancer
- D. cross-zone load balancing is not supported
- E. Elastic Load Balancer forwards traffic to primary private IP address (eth0 interface) on each instance

Answer (A,C,E)**Deployment****Question 1:**

What Amazon AWS service is available for container management?

- A. ECS
- B. Docker
- C. Kinesis
- D. Lambda

Answer (A)**Question 2:**

What is associated with Microservices? (Select two)

- A. Application Load Balancer
- B. Kinesis
- C. RDS
- D. DynamoDB
- E. ECS

Answer (A,E)**Question 3:**

Where does Amazon retrieve web content when it is not in the nearest CloudFront edge location?

- A. secondary location
- B. file server
- C. EBS
- D. S3 bucket

Answer (D)**Question 4:**

What two features of an API Gateway minimize the effects of peak traffic events and minimize latency?

- A. load balancing
- B. firewalls
- C. throttling
- D. scaling
- E. caching

Answer (C,E)

Question 5:

What three characteristics differentiate Lambda from traditional EC2 deployment or containerization?

- A. Lambda is based on Kinesis scripts
- B. Lambda is serverless
- C. tenant has ownership of EC2 instances
- D. tenant has no control of EC2 instances
- E. Lambda is a code-based service
- F. Lambda supports only S3 and Glacier

Answer (B,D,E)

Question 6:

How is code uploaded to Lambda?

- A. Lambda instance
- B. Lambda container
- C. Lambda entry point
- D. Lambda function
- E. Lambda AMI

Answer (D)

Question 7:

How are Lambda functions triggered?

- A. EC2 instance
- B. hypervisor
- C. Kinesis
- D. operating system
- E. event source

Answer (E)

Question 8: What three statements correctly describe standard Lambda operation?

- A. Lambda function is allocated 500 MB ephemeral disk space
- B. Lambda function is allocated 100 MB EBS storage
- C. Lambda stores code in S3
- D. Lambda stores code in a Glacier vault
- E. Lambda stores code in containers
- F. maximum execution time is 300 seconds

Answer (A,C,F)

Question 9: What network events are restricted by Lambda? (Select two)

- A. only inbound TCP network connections are blocked by AWS Lambda
- B. all inbound network connections are blocked by AWS Lambda
- C. all inbound and outbound connections are blocked
- D. outbound connections support only TCP/IP sockets
- E. outbound connections support only SSL sockets

Answer (B,D)

Question 10:

How is versioning supported with Lambda? (Select two)

- A. Lambda native support



- B. ECS container
- C. not supported
- D. Aliases
- E. replication
- F. S3 versioning

Answer (A,D)

Question 11: What is the difference between Stream-based and AWS Services when enabling Lambda?

- A. streams maintains event source mapping in Lambda
- B. streams maintains event source mapping in event source
- C. streams maintains event source mapping in EC2 instance
- D. streams maintains event source mapping in notification
- E. streams maintains event source mapping in API

Answer (A)

Question 12:

Select two custom origin servers from the following?

- A. S3 bucket
- B. S3 object
- C. EC2 instance
- D. Elastic Load Balancer
- E. API gateway

Answer (C,D)

Question 13:

What two attributes are only associated with CloudFront private content?

- A. Amazon S3 URL
- B. signed cookies
- C. web distribution
- D. signed URL
- E. object

Answer (B,D)

Question 14:

How are origin servers located within CloudFront (Select two)

- A. DNS request
- B. distribution list
- C. web distribution
- D. RTMP protocol
- E. source mapping

Answer (A,C)

Question 15:

Where are HTML files sourced from when they are not cached at a CloudFront edge location?

- A. S3 object
- B. origin HTTP server
- C. S3 bucket
- D. nearest edge location
- E. RTMP server
- F. failover edge location

Answer (B)

Question 16:

What is the capacity of a single Kinesis shard? (Select two)

- A. 2000 PUT records per second
- B. 1 MB/sec data input and 2 MB/sec data output
- C. 10 MB/sec data input and 10 MB/sec data output



D. 1000 PUT records per second

E. unlimited

Answer (B,D)

Question 17:

What Amazon AWS service supports real-time processing of data stream from multiple consumers and replay of records?

A. DynamoDB

B. EMR

C. Kinesis data streams

D. SQS

E. RedShift

Answer (C)

Question 18: Your company has asked you to capture and forward a real-time data stream on a massive scale directly to RedShift for analysis with BI tools.

What AWS tool is most appropriate that provides the feature set and cost effective?

A. DynamoDB

B. SQS

C. Elastic Map Reduce

D. Kinesis Firehose

E. SNS

F. CloudFront

Answer (D)

Question 19:

What feature permits tenants to use a private domain name instead of the domain name that CloudFront assigns to a distribution?

A. Route 53

B. CNAME record

C. MX record

D. RTMP

E. Signed URL

Answer (B)

Question 20:

What Amazon AWS service is available to guarantee the consuming of a unique message only once?

A. Beanstalk

B. SQL

C. Exchange

D. SQS

Answer (D)

Question 21:

What is the fastest and easiest method for migrating an on-premises VMware virtual machine to the AWS cloud?

A. Amazon Marketplace

B. AWS Server Migration Service

C. AWS Storage Gateway

D. EC2 Import/Export

Answer (B)

Question 22:

Select the stateless protocol from the following?

A. FTP

B. TCP

C. HTTP



D. SSH**Answer (C)****Question 23:****What are three valid endpoints for an API gateway?**

- A. RESTful API
- B. Lambda function
- C. AWS service
- D. web server
- E. HTTP method

Answer (B,C,D)**Question 24:****How is a volume selected (identified) when making an EBS Snapshot?**

- A. account id
- B. volume id
- C. tag
- D. ARN

Answer (D)**Question 25:****What deployment service enables tenants to replicate an existing AWS stack?**

- A. Beanstalk
- B. CloudFormation
- C. RedShift
- D. EMR

Answer (B)**Question 26:****What three services can invoke a Lambda function?**

- A. SNS topic
- B. CloudWatch event
- C. EC2 instance
- D. security group
- E. S3 bucket notification

Answer (A,B,E)**Question 27:****What two services enable automatic polling of a stream for new records only and forward them to an AWS storage service?**

- A. SNS
- B. Kinesis
- C. Lambda
- D. DynamoDB

Answer (B,C)**Question 28:** Your company is deploying a web site with dynamic content to customers in US, EU and APAC regions of the world. Content will include live streaming videos to customers. SSL certificates are required for security purposes. Select the AWS service delivers all requirements and provides the lowest latency?

- A. DynamoDB
- B. CloudFront
- C. S3
- D. Redis

Answer (B)**Question 29:****What are the advantages of Beanstalk? (Select two)**

- A. orchestration and deployment abstraction



- B. template-oriented deployment service
- C. easiest solution for developers to deploy cloud applications
- D. does not support cloud containers

Answer (A,C)

Question 30: You are a network analyst with JSON scripting experience and asked to select an AWS solution that enables automated deployment of cloud services. The template design would include a nondefault VPC with EC2 instances, ELB, Auto-Scaling and active/active failover. What AWS solution is recommended?

- A. Beanstalk
- B. OpsWorks
- C. CloudTrail
- D. CloudFormation

Answer (D)

Question 31:

Select two statements that correctly describe OpsWorks?

- A. Opsworks provides operational and configuration automation
- B. OpsWorks is a lower cost alternative to BeanStalk
- C. OpsWorks is primarily a monitoring service
- D. Chef scripts (recipes) are a key aspect of OpsWorks

Answer (A,D)

Question 32:

Your company has developed an IoT application that sends Telemetry data from 100,000 sensors. The sensors send a datapoint of 1 KB at one-minute intervals to a DynamoDB collector for monitoring purposes. What AWS stack would enable you to store data for real-time processing and analytics using BI tools?

- A. Sensors -> Kinesis Stream -> Firehose -> DynamoDB
- B. Sensors -> Kinesis Stream -> Firehose -> DynamoDB -> S3
- C. Sensors -> AWS IoT -> Firehose -> RedShift
- D. Sensors -> Kinesis Data Streams -> Firehose -> RDS

Answer (C)

Question 33:

Your company has an application that was developed and migrated to AWS cloud. The application leverages some AWS services as part of the architecture. The stack includes EC2 instances, RDS database, S3 buckets, RedShift and Lambda functions. In addition there is IAM security permissions configured with defined users, groups and roles.

The application is monitored with CloudWatch and STS was recently added for permitting Web Identity Federation sign-on from Google accounts. You want a solution that can leverage the experience of your employees with AWS cloud infrastructure as well. What AWS service can create a template of the design and configuration for easier deployment of the application to multiple regions?

- A. Snowball
- B. Opsworks
- C. CloudFormation
- D. Beanstalk

Answer (C)

Monitoring Services

Question 1:

What statement correctly describes CloudWatch operation within AWS cloud?

- A. log data is stored indefinitely
- B. log data is stored for 15 days
- C. alarm history is never deleted



D. ELB is not supported

Answer (A)

Question 2:

What are two AWS subscriber endpoint services that are supported with SNS?

A. RDS

B. Kinesis

C. SQS

D. Lambda

E. EBS

F. ECS

Answer (C,D)

Question 3:

What AWS services work in concert to integrate security monitoring and audit within a VPC? (Select three)

A. Syslog

B. CloudWatch

C. WAF

D. CloudTrail

E. VPC Flow Log

Answer (B,D,E)

Question 4:

How is CloudWatch integrated with Lambda? (Select two)

A. tenant must enable CloudWatch monitoring

B. network metrics such as latency are not monitored

C. Lambda functions are automatically monitored through Lambda service

D. log group is created for each event source

E. log group is created for each function

Answer (C,E)

Question 5:

What two statements correctly describe AWS monitoring and audit operations?

A. CloudTrail captures API calls, stores them in an S3 bucket and generates a Cloudwatch event

B. CloudWatch alarm can send a message to a Lambda function

C. CloudWatch alarm can send a message to an SNS Topic that triggers an event for a Lambda function

D. CloudTrail captures all AWS events and stores them in a log file

E. VPC logs do not support events for security groups

Answer (A,C)

Question 6:

What is required for remote management access to your Linux-based instance?

A. ACL

B. Telnet

C. SSH

D. RDP

Answer (C)

Question 7:

What are two features of CloudWatch operation?

A. CloudWatch does not support custom metrics

B. CloudWatch permissions are granted per feature and not AWS resource

C. collect and monitor operating system and application generated log files

D. AWS services automatically create logs for CloudWatch

E. CloudTrail generates logs automatically when AWS account is activated

Answer (B,C)



Question 8:

You are asked to select an AWS solution that will create a log entry anytime a snapshot of an RDS database instance and deletes the original instance. Select the AWS service that would provide that feature?

- A. VPC Flow Logs
- B. RDS Access Logs
- C. CloudWatch
- D. CloudTrail

Answer (D)

Question 9:

What is required to enable application and operating system generated logs and publish to CloudWatch Logs?

- A. Syslog
- B. enable access logs
- C. IAM cross-account enabled
- D. CloudWatch Log Agent

Answer (D)

Question 10:

What is the purpose of VPC Flow Logs?

- A. capture VPC error messages
- B. capture IP traffic on network interfaces
- C. monitor network performance
- D. monitor netflow data from subnets
- E. enable Syslog services for VPC

Answer (B)

Question 11:

Select two cloud infrastructure services and/or components included with default CloudWatch monitoring?

- A. SQS queues
- B. operating system metrics
- C. hypervisor metrics
- D. virtual appliances
- E. application level metrics

Answer (A,C)

Question 12:

What feature enables CloudWatch to manage capacity dynamically for EC2 instances?

- A. replication lag
- B. Auto-Scaling
- C. Elastic Load Balancer
- D. vertical scaling

Answer (B)

Question 13:

What AWS service is used to monitor tenant remote access and various security errors including authentication retries?

- A. SSH
- B. Telnet
- C. CloudFront
- D. CloudWatch

Answer (D)

Question 14:

How does Amazon AWS isolate metrics from different applications for monitoring, store and reporting purposes?



- A. EC2 instances
- B. Beanstalk
- C. CloudTrail
- D. namespaces
- E. Docker

Answer (D)

Question 15:

What Amazon AWS service provides account transaction monitoring and security audit?

- A. CloudFront
- B. CloudTrail
- C. CloudWatch
- D. security group

Answer (B)

Question 16:

What two statements correctly describe CloudWatch monitoring of database instances?

- A. metrics are sent automatically from DynamoDB and RDS to CloudWatch
- B. alarms must be configured for DynamoDB and RDS within CloudWatch
- C. metrics are not enabled automatically for DynamoDB and RDS
- D. RDS does not support monitoring of operating system metrics

Answer (A,B)

Question 17: What AWS service can send notifications to customer smartphones and mobile applications with attached video and/or alerts?

- A. EMR
- B. Lambda
- C. SQS
- D. SNS
- E. CloudTrail

Answer (D) Amazon Books • AWS Certified Solutions Architect

Associate Exam: Study Notes • AWS Certified Solutions Architect Associate

Exam: Certification Practice Questions (full answer key version)

Copyright 2018 - One Page WordPress Theme

