K21Academy
Learn Cloud from Experts

amazon web services

aws certified
Cloud Practitioner

AWS Certified Cloud Practitioner

50 SAMPLE EXAM QUESTIONS

[EDITION 01]

Contents

1 CLOUD CONCEPTS

Q1. Which of the below listed 2 design principles relates to the "Operational Excellence" pillar of the Well Architected framework? **(Choose 2)**

A. Implement a strong identity foundation
B. Enable traceability
C. Anticipate Failure
D. Manage change in automation
E. Perform operations as code

Answer: C, E

The operational excellence pillar of a well-architected framework has below 5 design principles. ● Perform operations as code

- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures

The security pillar of a well-architected framework has below 7 design principles.

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

The reliability pillar of a well-architected framework has below 5 design principles.

- Automatically recover from failure
- Test recovery procedures
- Scale horizontally to increase aggregate workload availability
- Stop guessing capacity
- Manage change in automation

Option A is INCORRECT Implement a strong identity foundation is the design principle relating to the security pillar.
Option B is INCORRECT. Enable traceability is the design principle relating to the security pillar.
Option C is CORRECT
Option D is INCORRECT Manage change in automation is the design principle related
option E is CORRECT

Reference:
https://k21academy.com/amazon-web-services/aws-solutions-architect/5-pillars-of-aws-wellarchitected-framework/

Q2. What is the ability of AWS products and services to recover from disruptions and mitigate disruptions known as

A. Resiliency
B. Consistency
C. Durability
D. Latency

Answer: A

Resiliency is the ability to recover from disruptions and mitigate disruptions.
Consistency involves more than one system storing information, to return the same result when queried.
Durability is the system's ability to perform even upon the occurrence of unexpected events.
Latency is typically the measurement of delay between request and response.

Option A is CORRECT as Resilience is the ability of AWS products to recover from disruptions and mitigate disruptions.
Option B is INCORRECT because Consistency ensures that similar results are returned by more than one system storing information, when queried.
Option C is INCORRECT because Durability is the ability of AWS product(s) to remain functional and perform despite unexpected events' occurrence.
Option D is INCORRECT because latency denotes the delay between getting a response after a request is made

Reference:
https://wa.aws.amazon.com/wat.concept.resiliency.en.html
https://wa.aws.amazon.com/wat.concept.consistency.en.html
https://wa.aws.amazon.com/wat.concept.durability.en.html
https://wa.aws.amazon.com/wat.concept.latency.en.html

Q3. An architect is asked to design a solution for a distributed system in which the system's components operate in a way that components of one system do not negatively impact other components of the system.
Which of the below listed architectural best practices can help to achieve this?

A. Request Throttling
B. using stateless services
C. Enabling automatic data backup
D. Implement loose coupling

Answer: D
The scenario in the question talks about a distributed system wherein there is minimal-to-no dependency amongst the components. This can be achieved by implementing loose coupling amongst the components.

Request throttling, and use of stateless services (Option A, B) help design resilient solutions for distributed systems that can withstand failures and can recover from failure quickly.

Enabling automatic data backup (Option C) is the best practice for failure management, as backups aligned with requirements will ensure the required recovery time objectives (RTO) and recovery point objectives (RPO).

Option A is INCORRECT because the scenario refers to ensure minimal dependency amongst the components. Request throttling does not ensure minimal dependency but helps build a resilient solution.
Option B is INCORRECT because using the stateless service ensures that the solution is resilient. However, loose coupling helps minimize the dependency amongst the various components in the solution
Option C is INCORRECT because implementing automatic data backup is a failure management best practice and does not contribute to minimize component dependency
Option D is CORRECT as loose coupling ensures that components are NOT tightly dependent on each other, assuring that if one component fails, it does not impact the working of other components.

Reference:
https://k21academy.com/amazon-web-services/aws-solutions-architect/5-pillars-of-aws-wellarchitected-framework/
https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

Q4. Which of the below statements is CORRECT regarding AWS Global infrastructure? A. Each AWS region has multiple Availability Zones

B. Many AWS regions has single availability zone
C. Availability zones are also known as AWS Local zones
D. To provide High Availability, AWS management console and control plane are isolated to a single region

Answer: A

Option A is CORRECT. The statement is Correct
Option B is INCORRECT. The statement is incorrect. Option A IS correct.
Option C is INCORRECT. The statement is incorrect Availability zones and AWS Local Zones are different.
Option D is INCORRECT The statement is incorrect. AWS management console and control plane utilize multi- AZs and are distributed across the AWS regions.
Reference:
https://k21academy.com/amazon-web-services/aws-solutions-architect/questions-and-answers/
https://aws.amazon.com/about-aws/global-infrastructure/ "Regions and AZs"

Q5. An online marketplace start-up dealing in real estate is planning to move to the cloud. Which of the below is NOT a benefit of moving to the cloud? A. Install on a company's own servers.

B. Go global in minutes.
C. Stop guessing capacity.
D. Benefit from massive economies of scale.

Answer: A

Option A is CORRECT. This description belongs to on-premises and is not a benefit of moving to the cloud.
Option B is INCORRECT. This is a benefit of moving to the cloud.
Option C is INCORRECT This is a benefit of moving to the cloud. Option
D is INCORRECT. This is a benefit of moving to the cloud.

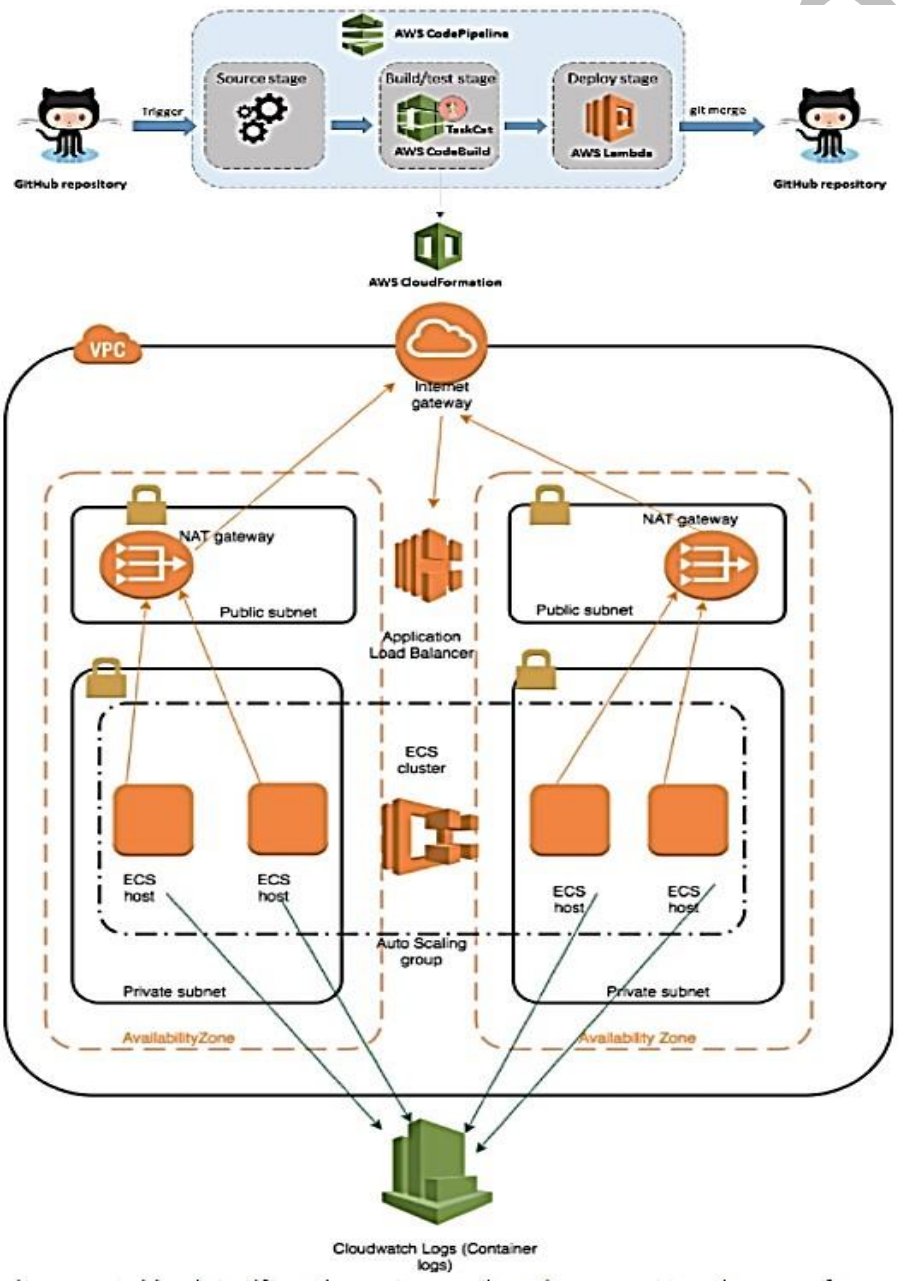
Reference:
https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloudcomputing.html

Q6. My On-Premises application's deployment cycle is roughly around 3-4 weeks. On refactoring this huge application, its features can be deployed on AWS cloud in a matter of 2-3 days. What is the benefit achieved by moving to the AWS cloud?

A. Elasticity
B. Flexibility
C. Agility
D. Resilience

Answer C

Explanation:



The scenario blends itself into the **Business Agility** value proposition where new features can be deployed faster to reduce errors The microservices architecture paradigm assists in Business Agility, where a large Monolith application is broken down into smaller functional units that can be developed & deployed faster AWS cloud, on the other hand, it provides services like Lambda, Elastic Container Services, Elastic Kubernetes Service that assists in developing & deploying microservices & deployment tools (CI/CD) like CodeBuild, CodePipeline for automating the deployment process. Combined, they provide an environment supporting an Agile Business.

Option A is incorrect. Elasticity is the ability to scale resources on demand whenever there is an increase in load on the existing infrastructure. This Value proposition will benefit in substantial cost savings where need not have to guess my capacity upfront

Option B is incorrect. Flexibility is the ability to utilize a broad range of products depending on the application & infrastructure demands. For example, there are a broad range of EC2 instance pricing models ranging from On Demand instances to Reserved Instances to Spot Instances and EC2 instance types Like General Purpose, Compute Optimized, Memory Optimized This will help with Low or No cost entries into the AWS cloud.

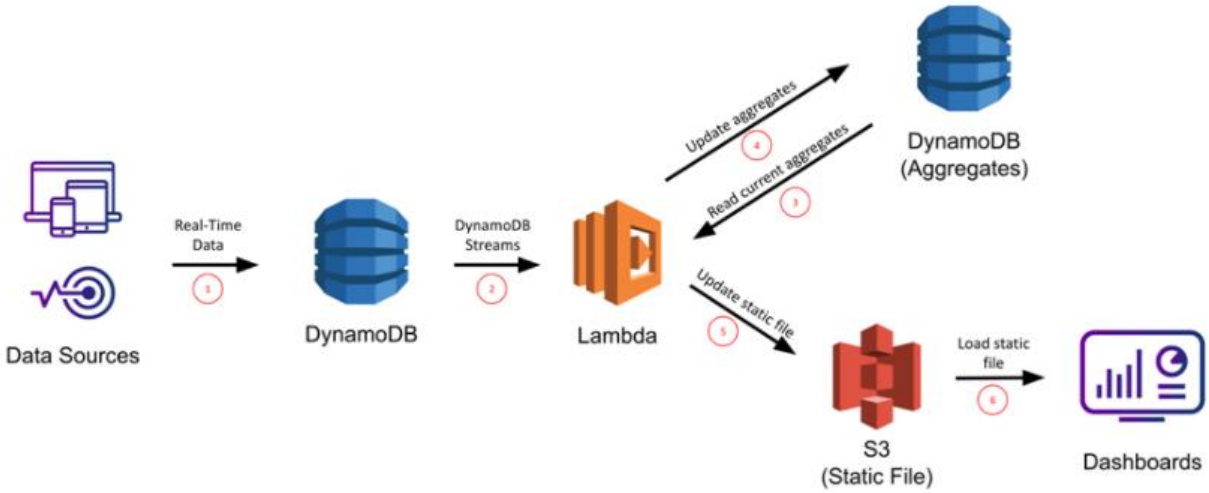
Option C is CORRECT. using an Agile environment provided by AWS Cloud, I can release application features much faster than a traditional On-Premises environment

Option D is incorrect. Operational resiliency results in the improvement of defined SLA's and reducing unplanned outages that would result in downtime The features of High Availability, Fault Tolerance gives rise to a resilient system.

Q7. I need to migrate millions of customers' financial transaction data from the On-Premise Mainframe system to a non-relational database in AWS. The database should also provide good performance for data retrieval and data analytics. Which of the following Database services is the most suitable?

A. Amazon RDS
B. Amazon RedShift
C. Amazon ElastiCache
D. Amazon DynamoDB

Explanation: On reading the scenario carefully, we notice that the Customer's Financial



transaction data is huge. It needs storage on the cloud. NoSQL databases like DynamoDB are designed to provide seamless scalability by automatically partitioning the database as it grows in size. So a NoSQL database like DynamoDB will be the most appropriate database service that can be used for the scenario.

Option A is incorrect. Here we are exclusively talking about Huge data volumes, Data retrieval and Data
analytics. RDS databases are most useful for heavy transaction processing systems. They also do not exhibit automatic partitioning capabilities with increased data volume & stream processing capabilities like a NoSQL database like DynamoDB provides.

Option B is incorrect. Amazon RedShift is a Data Warehousing solution primarily used for Operational analytics on business events. Data Warehouse may comprise a big collection of an Enterprise's structured & semi- structured data that can be used to build powerful reports & dashboards using Business Intelligence tools. Since we only have the Customer's transactional data for our scenario, RedShift will not be a good fit here.

Option C is incorrect. We are talking about the scenario for a data migration of On-Premise Mainframe data, which will require a permanent, secure data store for storing the highly sensitive Customer's financial data. Caching solutions are typically in-memory data stores used for

supporting applications requiring sub- milliseconds response times. Caching solutions usually maintain a subset of the data present in a data store that does not change frequently. Also, caching solutions do not provide any facility for performing real-time data analytics, although they provide the best performance compared to any other data storage solutions.

Option D is CORRECT. DynamoDB provides DynamoDB Accelerator (DAX) which is a fully managed, highly available in-memory cache. This will help us speed up the performance of data retrieval that we require. DynamoDB also has a feature called DynamoDB streams that enables real-time capture of data changes using event notifications. This helps applications to perform analytics on real-time streaming data to build dashboards without impacting database performance. The stream events are asynchronous in nature to consuming applications like a Lambda function. Since the Customer's transactional data is highly confidential & huge in volume, a robust, scalable, secure, performant data store like DynamoDB will be the best fit for our scenario.

References:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.Partitions.html
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html

Q8. I have certain applications On-Premises that run 24x7 & have a consistent load. I plan to move to the AWS Cloud. What is the economic feature that will benefit me most referred to?

A. Pay-as-you-go
B. Save when you Reserve
C. Pay less by using more
D. Pay-per-compute-time

Answer: B
From the scenario, we can see that the On-Premise's applications workload is continuous & stable. For these kinds of applications, it is easy to predict upfront capacity. Also, since the application runs continuously, I will benefit by reserving capacity for a certain period of time.

Option A is incorrect. The Pay-as-you-go model will be best used for workloads used for short durations & have unpredictable load. On-demand EC2 instances will be the best fit for this purpose.

Option B is CORRECT. Since there is continuous usage of these applications with a predictable load, it will be best for me to reserve capacity upfront (period of 1 - 3 years) that will provide a substantial discount of 30 - 50% compared to its On Demand counterparts.

Option C is incorrect. Pay less by using more refers to volume discounts provided by AWS for increased usage. E.g., S3 Standard provides the following storage pricing, also referred to as Tiered-Pricing.

Data Storage	Storage Pricing
First TB / month	$0.025 per GB
Next 450 TB / month	$0.024 per GB
Next 500 TB / month	$0.023 per GB

Option D is incorrect. Pay-per-compute-time refers to the use of serverless architectures like Lambda, where you pay only for the time when the compute resources are running. Unlike EC2 Pay-as-you-go pricing, AWS provisions resources for executing Lambda functions on the fly & removes them immediately after execution. So there is no idle utilization time that needs to be accounted for Since our scenario consists of long-running applications, this option will be impractical for usage.

References:
https://aws.amazon.com/pricing/#:-:text=AWS%200ffers%20you%20a%20pay,utilities%20like%20water%20and%20electricityhttps://d1.awsstaticcom/whitepapers/aws_pricing_overview.pdf

Q9. A client who has adopted AWS cloud services would like to ensure that his systems always scale with increasing traffic for a great end-user experience. I have implemented the same by defining Autoscaling Scale-In & Scale-Out policies & CloudWatch alarms that trigger the Autoscaling. Which Cloud Architecture Design principles have I implemented here? Select TWO most suitable options.

A. Encryption
B. Operational Excellence
C. Performance Efficiency
D. Cost Optimization
E. Least privilege

Answers: B and C
Looking at the scenario, a good end-user experience is attached to systems being performant with increasing load on them. A combination of Load balancing & Autoscaling enables a system to handle increase in load by spinning new instances to which the load will be distributed not to saturate resources like CPU & Memory on a single server instance. For the Autoscaling itself to

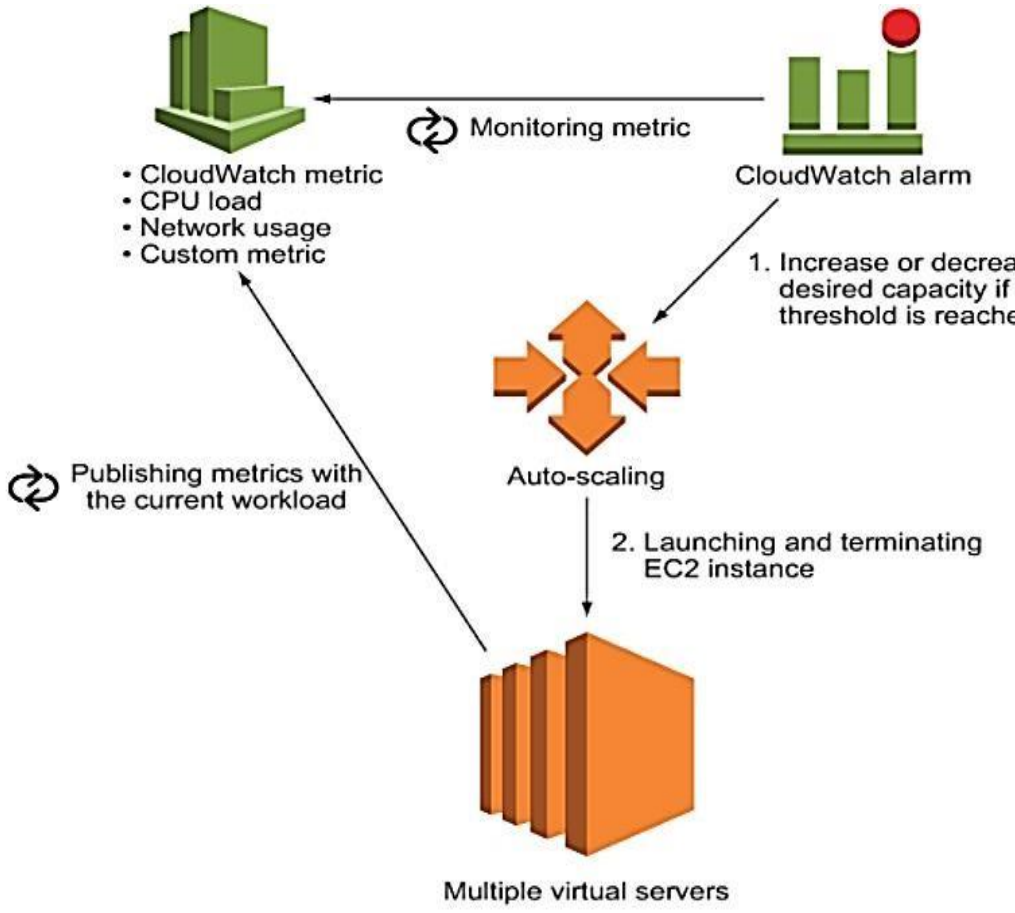
work efficiently, there needs to be a good monitoring system that can track resource utilization and enable automation. The scenario combines the Operational Excellence & the Performance Efficiency Architecture design principles.

Option A is incorrect. This scenario does not describe anything about data encryptions so that this option is not

Option B is CORRECT. The monitoring mechanism used here is CloudWatch for enabling Autoscaling to happen by tracking resource utilization metrics like CPU and Memory usage. The Operational Excellence pillar focuses on Monitoring systems that will deliver continuous business value by providing automation, responding to events within the system. In our scenario, automating the system's Scalability through monitoring will help maintain the desired performance levels.

Option C is CORRECT. The Performance Efficiency pillar focuses on monitoring the performance of a system. CloudWatch metrics help monitor a system's performance by using metrics like CPU, Memory, Disk utilization etc... Automating tasks like AutoScaling using CloudWatch Alarms and defining scaling policies will ensure that the client's performance requirements will always be met when there is an increase in traffic.

Option D is incorrect. In spite of using Scale-in & Scale-out policies, I can be benefitted from cutting down idle resource utilization costs. The scenario deals more with Performance & Operational aspects.
Option E is incorrect. Least privilege is a security principle which is not mentioned in the question.



Q10. A customer's Data center and its applications are connected to AWS using a dedicated network (Direct Connect). What is the Cloud deployment model?

A. Public Cloud
B. Multi Cloud
C. Private Cloud
D. Hybrid Cloud

Answer: D

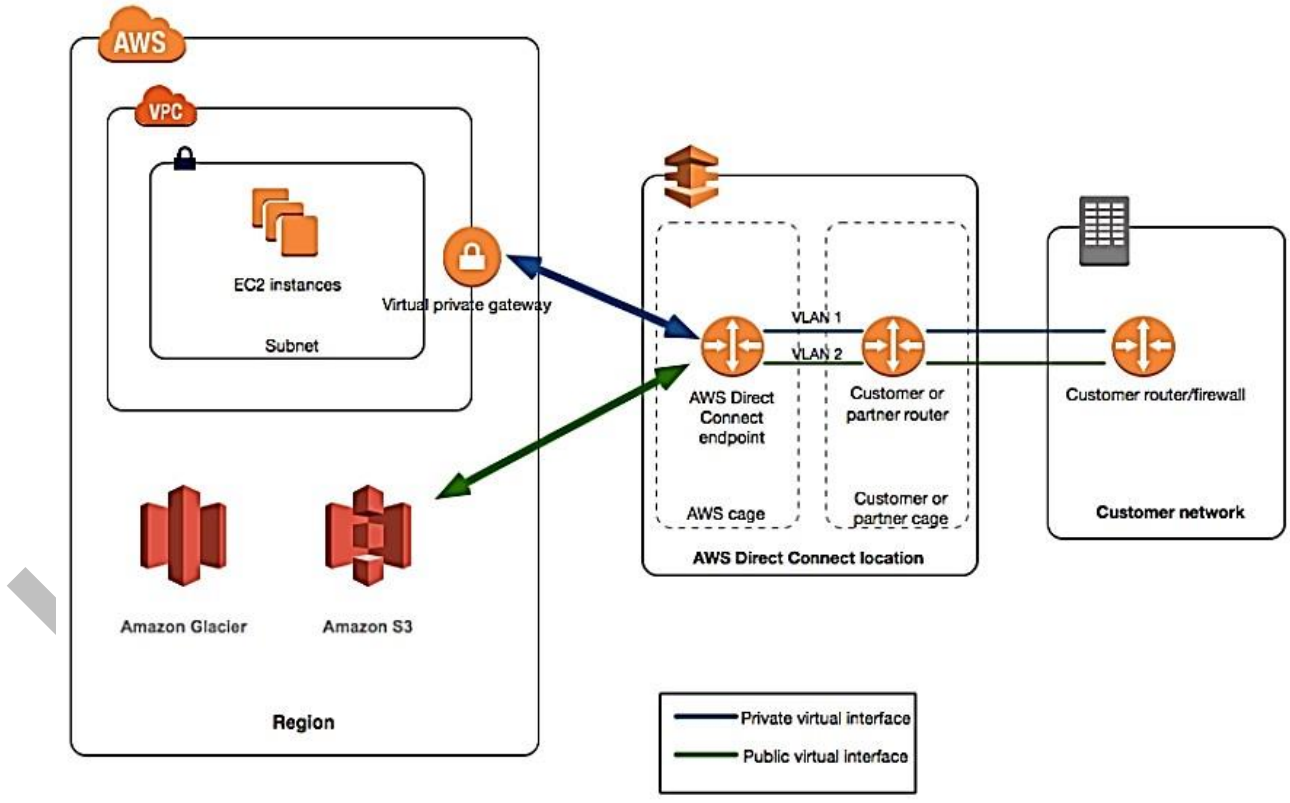
Option A is incorrect. When an application is fully deployed on a vendor's (AWS, Google Cloud) Cloud Infrastructure, it is termed as a Public Cloud. The application features may have been either developed on the cloud (Cloud Native) or migrated from an existing Client's On-Premises infrastructure. Our scenario uses both the Customer's Data Center and AWS.

Option B is incorrect. A multi-cloud leverages different Cloud Provider's environments. He may deploy his applications on AWS and Google Cloud-based on compute speed requirements, availability of managed services etc. With the use of Multi-Cloud, it is best to use Open Source tools like Terraform for Infrastructure as Code, Splunk for monitoring that are cloud

vendoragnostic to avoid vendor lock in. Since our scenario uses only the Customer's Data Center and AWS, there are no multiple cloud deployments.

Option C is incorrect. A Private Cloud refers to a cloud environment that has been built In house on the Client's premises using Virtualization and resource management tools. Private clouds are usually built for specific security and regulatory requirements, especially hardware or configuration requirements, and extremely critical network latency that may not be possible on a vendor's public cloud platform. Since our scenario has both the Client's data center & the AWS Cloud, it will not result in a Private Cloud configuration.

Option D is CORRECT. The cloud deployment model is a Hybrid Cloud. Hybrid clouds are often used where there is a requirement of burst capacity where workloads are "spilled over" to a different cloud environment to meet capacity demands for a short period of time. Here, purchasing capacity may not be a good idea since it will be extremely ineffective from a cost standpoint resulting in underutilization of resources once the requirement for capacity ends. The other compelling use case for a Hybrid cloud is a Highly Available / Disaster Recovery environment where the cloud model offers a lot of flexibility in making resources in the event of a Datacenter failure where the client may not need upfront investments for resources for an alternate site.



Q11. Which of the following may NOT be an Economic benefit to a client using AWS cloud services?

A. The Client is running a dedicated MySQL Database Server on AWS with his own CPU bound license (BOYL).
B. The Client is running Spot Instances for batch data processing workloads.
C. The client is running applications with a relatively predictable & consistent resource Demand using AWS Reserved Instances.
D. The client is using S3 Intelligent Tiering storage class while uploading objects.
E. The client is using an Active - Passive failover routing strategy of his On - Premise Data Center to AWS cloud.

Answer: A

Option A is CORRECT. CPU bound software Licenses Will require a Dedicated Host tenancy model rather than a Shared tenancy model for the EC2 instances hosting the MySQL Database software Dedicated hosts are the most expensive tenancy model when it comes to pricing. For example, An m4 large On Demand dedicated host is 24 times more expensive than an Ondemand shared host. A dedicated host tenancy may be used under exceptional circumstances of spiky traffic. while purchasing Hardware On-Premises may not be the best option. Then the client can take advantage of Cloud Elasticity

Option B is incorrect. Batch processing jobs rely more on accuracy rather than on speed which forms a good use case for using Spot Instances. providing economies of compute where intermittent disconnections may not be a real problem.

Option C is incorrect. AWS Reserved Instances have discounts on the EC2 usage This method can provide economic benefits.

Option D is incorrect. S3 Intelligent Tiering is a smart solution for managing the lifecycle of S3 objects resulting in economies of cost. With intelligent tiring, there are no retrieval fees nor there are any fees for moving objects between tiers unlike using S3 lifecycle policies which incurs data transfer charges. S3 lifecycle policies are also often challenging to define due to the unpredictable nature of application adoption and usage. Even in scenarios where access frequency is known, it may so happen that customers may not use proper storage class adjustments resulting in nonoptimized budgets.

Option E is incorrect. An Active-Passive failover will always be economical to a client using the strategy for Disaster Recovery scenarios since he will not be investing in an entire redundant site with all resources running simultaneously. He will have the flexibility to select his strategy depending on his Recovery Time objectives. This will help him to save on costs.

References:
https://aws.amazon.com/ec2/dedicated-hosts/pricing/
https://aws.amazon.com/ec2/pricing/on-demand/

Q12. Among the AWS resources or the AWS features (cloud concepts) Listed below, which option does NOT provide automation capabilities?

A. Elastic Beanstalk
B. DynamoDB
C. Fault Tolerance
D. RDS manual snapshot

Answer: D

Option A is incorrect. Elastic Beanstalk provides a fast way to deploy a web application on AWS. Behind the scenes, it automatically handles resource provisioning, load balancing, autoscaling and monitoring when Configured.

Option B is incorrect. DynamoDB contains a feature called DynamoDB streams that provides change events for automatically capturing data during operations like CREATE, DELETE, and UPDATE on its tables. This relieves application developers from implementing naive methods like using a timer at regular intervals to scan the tables for specific data patterns for creating dashboards, which is non-real-time, performance-intensive and costly since it Will use Read Capacity Units (RCCJ). The events can be subscribed by a Lambda function, its resulting data patterns extracted in real-time without impacting Table performance or costs.

Option C is incorrect. Fault tolerance environment always ensures that catastrophic loss of resources like Data Centers or Availability zones will not result in application downtime resulting in 100% availability. Fault tolerance mechanisms always have an Active-Active site failover mechanism where both the Primary and Backup resources are fully functional and operational. Traffic is sent to both the sites, and in the event of failover, traffic will be routed to the available site. Fault-Tolerant setups may have different scenarios like Disaster Recovery, Multi-AZ database setups exhibiting redundancy with 2 copies of data to ensure write availability and 3 copies of data to ensure read availability. We may compare Fault Tolerance to an Aircraft analogy where the loss of an engine will still allow the plane to function without rectifying it, which won t be possible mid-air.

Option D is CORRECT. Unlike automated backups, manual snapshots are taken by users when needed. It IS not an automation method.

References:
• https://aws.amazon.com/blogs/database/dynamodb-streams-use-cases-and-design-patterns/

Q13. I have certain applications On-Premises that experience times within a year where infrastructure takes a heavier load impact (e.g., Christmas, Thanksgiving, etc.) than other times in the year. You do not want to decommission the on premises infrastructure. What is the easiest and most cost-effective way in which I can handle this load?

A. By moving all my infrastructure to AWS Cloud and using On-Demand capacity
B. By creating a Private Cloud environment in my On-Premises data center that will provide me with the required elasticity
C. By using Scheduled Reserved Instances to match capacity reservation for the load
D. By provisioning Burst Capacity on the AWS Cloud for the duration of the load

Answer: D

Option A is incorrect. On looking at the scenario, we see that the variable load is only for a specific duration of time. So moving the infrastructure entirely to a Public Cloud will not be the best solution to gain maximum benefit out of the elastic nature of a Public Cloud.

Option B is incorrect. A Private Cloud will be more beneficial where there is a consistent load rather than a variable load. It will be good to have a Private Cloud hosting the applications for economies of cost and agility rather than elasticity, which can be best obtained using a Public Cloud.

Option C is incorrect. Reserved Instances are usually best chosen where there is consistent usage and predictable load for a certain duration of time (1-3 Years). Scheduled Reserved Instances have the ability to reserve capacity for a predictable recurring schedule that may be in a day, week, or month. The advantage here is w.r.t the costs that I Incur for Reserved Instances that can be managed without paying everything upfront rather than elasticity

Option D is CORRECT. This is the best way to reduce the costs of purchasing Hardware and getting the benefits of the elasticity and On-Demand pricing provided by a Public Cloud environment. On these specific occasions, I can demand a burst capacity by going to the AWS Public cloud. That will certainly help me maintain the performance of my applications at heavy load. Once the load reduces, I can then terminate the instances that are no longer used to save costs.

References:
https://docs.awsamazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html

2 TECHNOLOGY

Q1. Which AWS service is a machine learning-based tool that analyzes metrics of historical utilization and makes recommendations of compute service(s) to be used for the workload?

A. AWS Outposts
B. AWS Well-Architected Tool
C. AWS Management Console
D. AWS Compute Optimizer

Answer: D

Option A is INCORRECT because AWS Outpost is a fully managed service that provides a seamless hybrid experience by facilitating the running of AWS services and infrastructure onpremises. AWS outpost does not provide recommendations for using the compute services after analyzing the past utilization metrics.

Option B is INCORRECT as AWS Well-Architected Tool is a tool that provides advice on architecting the workload in the cloud. This tool also enables customers to review their architecture against the best practices.

Option C is INCORRECT because AWS Management Console is a web-based user interface that helps users to access and manage all the aspects of all the available AWS services. This is a management and governance tool.

Option D is CORRECT. AWS Compute Optimizer is a machine learning-based tool that analyzes metrics of historical utilization and makes recommendations of compute service(s) to be used for the workload.

Reference:
https://aws.amazon.com/outposts/
https://aws.amazon.com/well-architected-tool/
https://aws.amazon.com/console/
https://aws.amazon.com/compute-optimizer/

Q2. Which of the below could be used to perform best practices aligned deployment of popular technologies on AWS, and eventually reduce the time taken for environment build and eventual usage of the environment?

A. AWS Elastic Beanstalk
B. AWS OpsWorks
C. AWS Auto deploy
D. AWS Quick Starts

Answer: D

Option A is INCORRECT. AWS Elastic Beanstalk helps in web applications and services scaling and deployment. However, we need to provide the code.

Option B is INCORRECT. Aimed specifically for chef and puppet, AWS OpsWorks helps facilitate managed instances of Chef and Puppet.

Option C is INCORRECT. AWS Auto deploy is an Invalid service.

Option D is CORRECT. AWS Quick Starts: Built by AWS Architects and partners, quick start helps to automate deployments aligned with the best practice. CloudFormation templates are included along with Quick Start for the automation of the deployment.

Reference:
https://aws.amazon.com/elasticbeanstalk/
https://aws.amazon.com/opsworks/
https://aws.amazon.com/quickstart/

Q3. A developer working on enhancing a few applications in AWS requires an AWS service that can host glt-based repositories securely. Which AWS service can the developer use?

A. AWS CodeCommit
B. AWS CodeStar
C. Amazon CodeGuru
D. AWS CodePipeline

Answer: A

Option A is CORRECT. AWS CodeCommit helps in hosting git-based repositories securely. AWS CodeCommit IS a fully managed service and provides source control services.

Option B is INCORRECT. AWS CodeStar is a cloud-based AWS service that helps in swift and quick development and building and deploying applications in AWS.

Option C is INCORRECT. Amazon CodeGuru is an ML-powered development tool that provides code quality improvement recommendations.

Option D is INCORRECT. AWS CodePipeline is a fully managed workflow management tool that facilitates automation of various phases of the release process.

Reference:
https://aws.amazon.com/codecommit/
https://aws.amazon.com/codestar/
https://aws.amazon.com/codeguru/
https://aws.amazon.com/codepipeline/

Q4. Which of the below statements are true with regards to Amazon S3 security and access management? **Choose 2**.

A. Self-created S3 resources are only accessible to the user by default.
B. Access Control Lists (ACLs) could be used to grant time bound access using temporary URLs.
C. By default, S3 buckets are private, however, objects are public. The object owner needs to change the permissions upon creation of objects to make the objects private. D. Amazon Macie can protect data in Amazon EC2.
E. Server-side and client-side encryptions are supported by S3 for data uploads.

Answer: A, E
Option A is CORRECT. Users, by default, have access only to the S3 resources that they have created.
Option B is INCORRECT. Time-bound access using temporary URLs can be provided using query string authentication.
Option C is INCORRECT. By default, both S3 buckets and objects are private.
Option D is INCORRECT. Amazon Macie is a tool to protect the data n Amazon S3 instead of EC2.
Option E is CORRECT. S3 supports both server-side and client-side encryptions.

Reference:
https://k21academy.com/amazon-web-services/amazon-s3-bucket-and-storage-classes/
https://aws.amazon.com/s3/security/

Q5. An e-commerce company has launched a new application and determined that it needs to perform load distribution for http and https traffic because of the increased traffic during the monthly discount days. Which Load Balancer would be suitable?

A. Classic Load Balancer B.
Legacy Load Balancer
C. Application Load Balancer
D. Network Load Balancer

Answer: C

Option A is INCORRECT. Classic Load Balancer operates at request and connection level and provides basic load balancing.

Option B is INCORRECT. Legacy Load Balancer is an invalid option.

Option C is CORRECT. Application Load Balancer is apt for http and https traffic load balancing. Application load balancer operates at layer 7.

Option D is INCORRECT. Network Load Balancer is apt for TCR UDP, TLS traffic load balancing and helps provide extreme performance.
Reference:

https://aws.amazon.com/elasticloadbalancing/

Q6. Which of the following statements related to the AWS Global Infrastructure are correct? Select the best TWO.

A. For achieving High Availability and Performance, customers usually deploy their applications across multiple AWS Regions
B. Edge locations can be used to deploy infrastructures like EC2 instances, EBS storage
C. Availability zones can contain one or more data centers.
D. An EC2 instance's AMI in a particular region can be copied to another region for using it in that Region.
E. An elastic IP address is allocated to an Availability Zone

Explanation:
Answers: C and D
Option A is incorrect because the first level of redundancy is always Availability Zones when it comes to High Availability & Performance. When applications are deployed across multiple Availability Zones within the same region, a single Availability Zone's failure will not result in the application being unavailable as the failover mechanism will switch the request of a client to another availability zone. When requests are routed through a load-balancer, it will manage requests depending on the resource utilization of services within an availability zone. This will ensure the good performance of the application. Regional replications are a second level of redundancy where data is replicated between Geographical Regions. One of the reasons could be a Disaster Planning architecture for Business Continuity where a complete Region becomes unavailable & a backup of the data can be maintained in another region for redundancy.

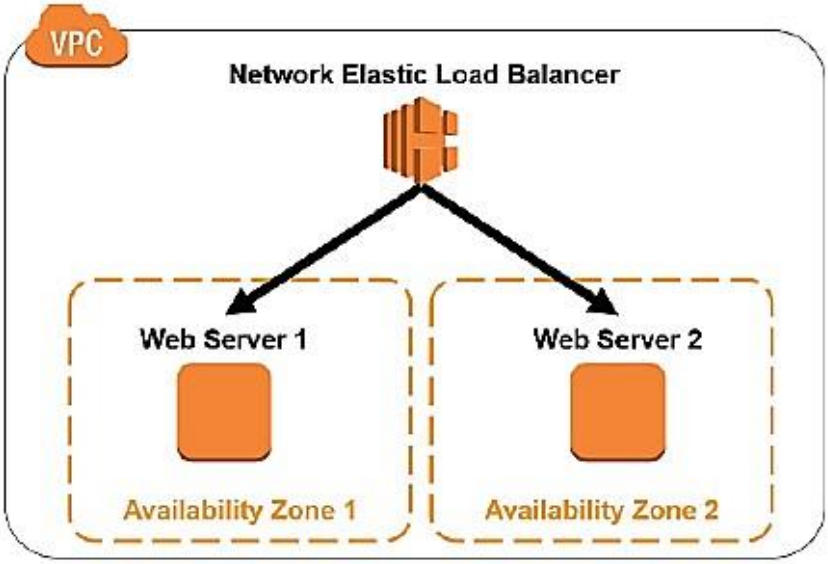
Option B is incorrect. Edge locations are used by services like CloudFront to cache data & reduce latency for end-user access by using those Edge locations as a Global Content Delivery Network (CDN). EC2 instances can be used as Origin servers to a CloudFront distribution for serving dynamic content.

Option C is CORRECT. An Availability Zone is a logical Data Center within a Region. Each zone in a Region has redundant and separate power, networking and connectivity to reduce the likelihood of two zones failing simultaneously. Each zone could be backed with one or more physical Data Centers, the largest being backed by 5.

Option D is CORRECT. Copying an AMI from one region to another enables you to launch consistent instances based on the same AMI to different Regions. The consistency can be observed from the fact that the AMI's can contain pre-installed software that can be used in different regions. For example, if I have a redundant AMI copy as a backup in another Region, it becomes easy to launch an EC2 instance from that AMI in that Region without reinstalling all that software again, thus improving downtime of my applications.

Option E is incorrect. Elastic IP (EIP) addresses are static IP addresses that can be created and assigned within an AWS Account rather than an Availability Zone. You can have a maximum of 5 EIP's for an Account. It can be assigned to an EC2 instance. An EIP is most useful for an application hosted on a single EC2 instance with its IP mapped to a domain name. When the EC2 instance has a public IP & getting restarted, it will be assigned a new public IP making the site unavailable unless it is remapped to the domain. An EIP will help here by retaining the same public IP address at the time of a server restart so that the site does not incur downtime

Diagram:



Reference:
https://aws.amazon.com/about-aws/global-infrastructure/?p=ngi&loc=0
https://aws.amazon.com/blogs/aws/ec2-ami-copy-between-regions/

Q7. Which of the following AWS automation services does NOT provide the capability of provisioning IT infrastructure and deployment of applications?

A. AWS CodePipeline
B. AWS CloudFormation
C. AWS Elastic Beanstalk
D. All of them provide both provisioning of IT infrastructure & deployment of applications

Answer: A

Option A is CORRECT. CodePipeline is a Continuous Integration / Continuous Delivery service that builds, tests & deploys code whenever there is a change in the source code. CodePipeline does not in itself provision IT infrastructure. instead it uses available targets like ECS S3, Elastic beanstalk for deploying generated artifacts.

Option B is incorrect. AWS CloudFormation provides an easy way to model a collection of AWS resources, provision them quickly and consistently and manage them throughout their Lifecycle by treating infrastructure as code. Organizations with complex infrastructures benefit from CloudFormation, where templates describe desired resources & their dependencies. They can be used to launch & configure them as a stack rather than configuring resources manually which can be extremely time-consuming & error-prone Templates can be used to create, update, and delete an entire stack as a single unit, as often as needed. You can manage and provision stacks across multiple AWS accounts and AWS Regions.

Option C is incorrect. Elastic beanstalk lets you provision resources & deploy a web application in a matter of minutes. Elastic Beanstalk handles your hosting environment's details and allows you to define Capacity provisioning, Load balancing. scaling & application health monitoring for your applications. When you deploy your web application, Elastic beanstalk provisions a set of AWS resources, including EC2 instances. alarms, Security groups etc.

Option D is incorrect since CodePipeline does not provision resources.

Reference:
https://k21academy.com/amazon-web-services/deploy-aws-codepipeline/
https://aws.amazon.com/codepipeline/ https://aws.amazon.com/cloudformation/
https://aws.amazon.com/elasticbeanstalk/

Q8. I have an application whose execution time is short but is very critical. For keeping my costs minimum for running the application, what is the best AWS Compute service that I can use?

A. Spot Instance
B. Lambda function
C. Reserved Instance
D. On demand EC2 Instance

Answer: B

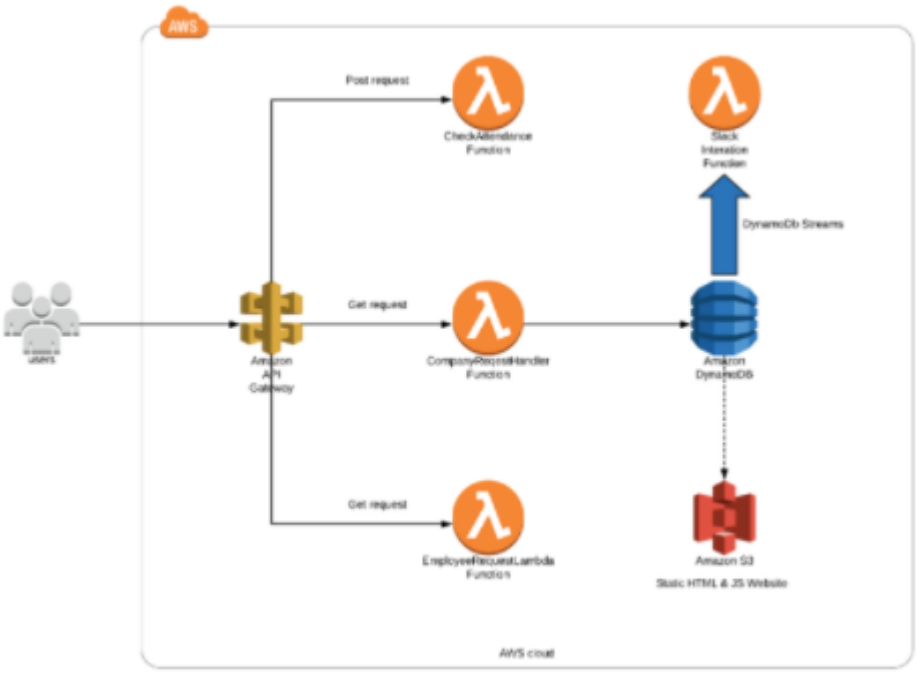
Option A is incorrect. Although spot instances offer very low compute prices, they are most useful in situations where you have flexible start & end times for your applications. Since time criticality is an important aspect for application execution, spot instances may not be the best fit here which can be terminated within a short notice period.

Option B is CORRECT. With AWS lambda, code gets executed only when needed & AWS automatically takes care of dynamically provisioning/deprovisioning compute capacity to execute the Lambda function. Also known as serverless computing technology, users pay only for the duration of the lambda function execution & they do not need to provision or manage servers. This is the best possible way to dramatically reduce costs without managing idle time of unused compute capacity.

Option C is incorrect. Although Standard Reserved Instances provide up to 75% off on-demand price, they are more useful for steady-state or predictable applications. Since our scenario only talks about limited usage, RI may not be a good choice.

Option D is incorrect. On-demand EC2 instances need to be provisioned & managed by the user. You also need to account for idle compute time & terminate instances that are idle which otherwise will have cost implications.

Diagram: Depicts a serverless architecture using API Gateway, Lambda, Dynamo DB streams for an Employee Attendance system.



.

Reference:
https://d1.awsstatic.com/whitepapers/serverless-architectures-with-aws-lambda.pdf
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html
https://aws.amazon.com/lambda/
https://aws.amazon.com/ecs/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc&ecs-blogs.sort-by=item.additionalFields.createdDate&ecs-blogs.sort-order=desc

Q9. I have some data that is not frequently accessed. But when requested within six months, the data needs to be available immediately. After six months, the data is not accessed but needs to be maintained for historical purposes. What is the best S3 storage class lifecycle available to me with the lowest possible cost?

A. Store data for the first 6 months in S3 Standard & move data to Glacier after that.
B. Store data the first 6 months in S3 One Zone - IA & move data to Glacier after that.
C. Store data the first 6 months in S3 Standard IA & move data to Glacier after that.
D. Store data in Glacier & use expedited retrieval for accessing data immediately.

Answer: B

On analyzing the scenario carefully, we can see here that data is infrequently accessed for the first 6 months & is then archived for long term storage

Option A is incorrect since it is not advisable to store data in S3 Standard that is not frequently accessed. S3 standard will incur higher costs for this scenario.

Option B is CORRECT. S3 One Zone IA offers the best cost-effective solution for infrequently accessed data. Since the lowest cost is desired here, we can overlook the resilience model offered by High Availability storage solutions. After six months, data can be moved to Glacier for archival purposes.

Option C is incorrect. S3 Standard IA is more cost-effective than its S3 standard counterpart for infrequently accessed data. But we do not select it as the best available option compared to the pricing of S3 One Zone IA, which offers a 20% subsidized cost compared to S3 Standard IA.

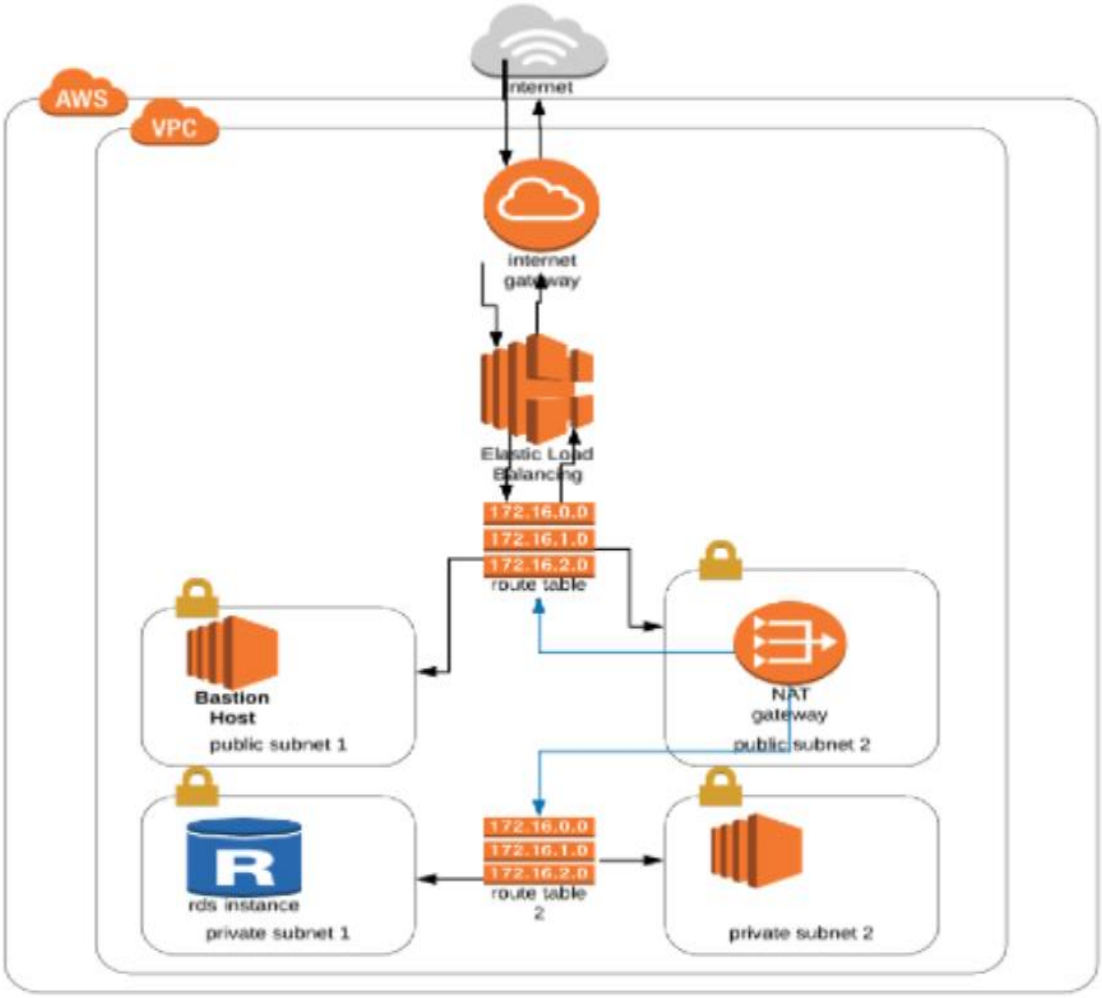
Option D is incorrect because Glacier offers a way to store archival data rather than storing it for frequent/infrequent access. Also, expedited retrieval costs are greater (0.03 per GB) than the S3 One Zone IA cost which is 0.01 per Ga.

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

Q10. I have a Virtual Private Cloud infrastructure environment hosting an Application & a Database. What are the best practices that can be used to host them within the infrastructure? Select TWO.

A. Host the Application in a Public Subnet, Database in a Private Subnet with an ELB front ending the Application in a Public Subnet
B. Host both the Application & Database in a Private subnet with an ELB front ending the Application in a public Subnet
C. Host both the Application & Database in a Public subnet with an ELB front ending the Application in a public Subnet
D. Subnet configured for the Application should have a route to the Internet Gateway E. Subnet configured for the ELB should contain a NAT Gateway

Answers: B and E



Option A is incorrect. The entry point to the Application is the ELB. Its best to have only the ELB within the Public Subnet and have the Application & Database in the Private subnet. This way, a user can access the application through the ELB to provide High Availability & failover.

Option B is CORRECT. This is the best possible configuration that can be defined for maximum Security, High Availability & Failover.

Option C is incorrect. This configuration will be least Secure since users will be able to access all the Application, Database & ELB within the Public Subnet. Also, single points of failure may occur due to a Lack of proper services structuring within the respective layers.

Option D is incorrect since the Application should be placed within the Private Subnet that should not route the Internet Gateway. Instead. it should have a route to the NAT gateway for accessing the Internet in an Egress manner.

Option E is CORRECT. A NAT gateway allows resources hosted within the Private Subnet to access the Internet for operations like OS updates or DB patch updates. Since the ELB is the only resource within a Public Subnet, it should ideally contain a NAT Gateway that will allow the Application or Database to access the Internet.

Diagram: The figure below shows a typical configuration of an ELB. EC2 instance. ADS. NAT Gateway, Bastion host & route table. The NAT Gateway & Bastion Host is contained within the Public Subnet along with the ELB, while the EC2 instance & RDS is contained within a Private Subnet

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

Q11. I have two applications, “Image Processing” & “Order Processing,” hosted on my website on different EC2 servers in an Auto Scaling Group. What is the best way to provide access to a user for any of these applications on this website?

A. I can provide the public DNS URL of each of my servers where my application is Hosted.
B. I can use the Classic Load Balancer that will route requests to different applications depending on the user’s request.
C. I can use the Application Load Balancer that will route requests to different applications depending on the user’s request. A
D. I can use the Network Load Balancer that will route requests to different applications depending on the user’s request.

Explanation:
Answer: C

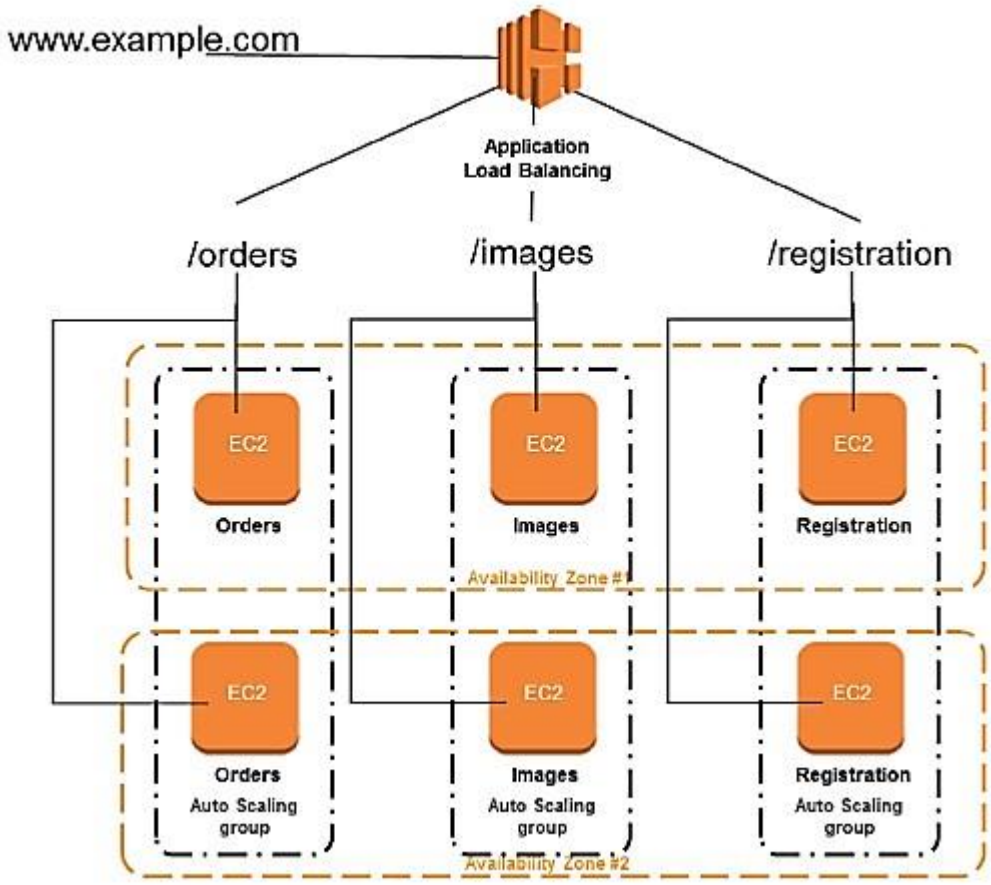
1. It will be inefficient & cumbersome having the users to know many URLs or IP addresses as the number of applications increase.
2. Load distribution will not be possible with this scenario resulting in possible Single Point of Failures & unacceptable application performance as the load increases.
3. High Availability & failover will not be possible since we are exposing a static IP address or URL.

Option B is incorrect. Classic Load Balancer provides basic load balancing capabilities that will distribute traffic equally among many servers under it.
Option C is CORRECT. Application Load Balancer supports a feature named Path-based routing that will route requests based on URL patterns provided in the request. Application Load Balancer achieves this feature by using Target groups that hold a specific set of resources. EC2 instances, Auto Scaling groups, ECS tasks etc. It is the responsibility of the Target group which

keeps track of the instances of that particular class and intelligently route requests based on the load within a specific group.

Option D is incorrect. Network Load balancers distribute load based on network variables like IP address, destination ports. It is layer 4 (TCP) and below and is not designed to take into consideration anything at the application layer such as content type, cookie data, custom headers, user location, or the application behavior. So Network Load balancer cannot ensure the availability of applications.

Diagram:
As seen in the diagram below, the Application Load Balancer acts as a single point of entry to various applications hosted on a website. Based on the URL pattern,
e.g., www.example.com/orders, the ALB will route the request based on the Path to a specific Target Group hosting the application. In this case, the Orders Auto Scaling group will be held by the ALB's Target Group. Within the Auto Scaling group, the ALB will intelligently route the request to different server instances depending on the load.



References:
https://aws.amazon.com/elasticloadbalancing/#:~:text=Elastic%20Load%20Balancing%20automatica
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html
https://docs.aws.amazon.com/autoscaling/plans/userguide/what-is-aws-auto-scaling.html

Q12. I need to keep track of all invalid login attempts of a user when he tries to SSH to an EC2 instance. How can I achieve that?

A. Collecting log data from the EC2 instance and delivering them to a CloudWatch Logs log stream.
B. Integrating CloudTrail with CloudWatch Logs to deliver data events captured by the login activity to a CloudWatch Logs log stream.
C. Running a log utility on the EC2 instance periodically and checking the server logs.
D. Both B & C.

Answer: A

Option A is CORRECT. Log data can be collected from EC2 instances by installing & configuring a CloudWatch Log Agent on the EC2 server. These logs can then be delivered to CloudWatch log group streams, where they can be analyzed using Metric Filters. Actions like notifying an admin on the invalid login attempt can then be done by defining CloudWatch alarms on the associated Log metrics.

Option B is incorrect. CloudTrail tracks API requests made by users. Its logs will be more useful when operations on resources are performed like creating an EC2 instance or terminating an EC2 instance. Those logs can be integrated with CloudWatch for detecting abnormal operations on different AWS resources. The user login scenario is captured as logs on the EC2 instance & sent to CloudWatch by the Log Agent. When a user tries to SSH to an EC2 instance, the activity is not recorded in AWS CloudTrail as it is not an AWS API call.

Option C is incorrect. Although it is possible to run a log utility to report failed login attempts by the user, it defeats the advantages that a centralized Monitoring & Logging system offers. Also, by doing so, real-time monitoring will not happen due to the absence of streaming data resulting in delayed incident detection & resolution.

Option D is incorrect since the best way to track log data is to push it to a Log stream destination where it can be quickly monitored resulting in faster incident resolution.

Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html
https://aws.amazon.com/cloudwatch/
https://aws.amazon.com/cloudtrail/

Q13. I am using the Amazon Simple Notification Service to send notifications to alert admins whenever the CPU utilization of an EC2 instance crosses 70%. Which of the following can be subscribers to an SNS Topic? Select TWO.

A. Email
B. S3
C. Lambda
D. CloudWatch
E. DynamoDB Stream

Answers: A and C

SNS is extremely useful for fan-out type of applications, i.e. Multiple clients that push messages to an SNS topic & multiple listeners can be notified when a message arrives at the Topic.

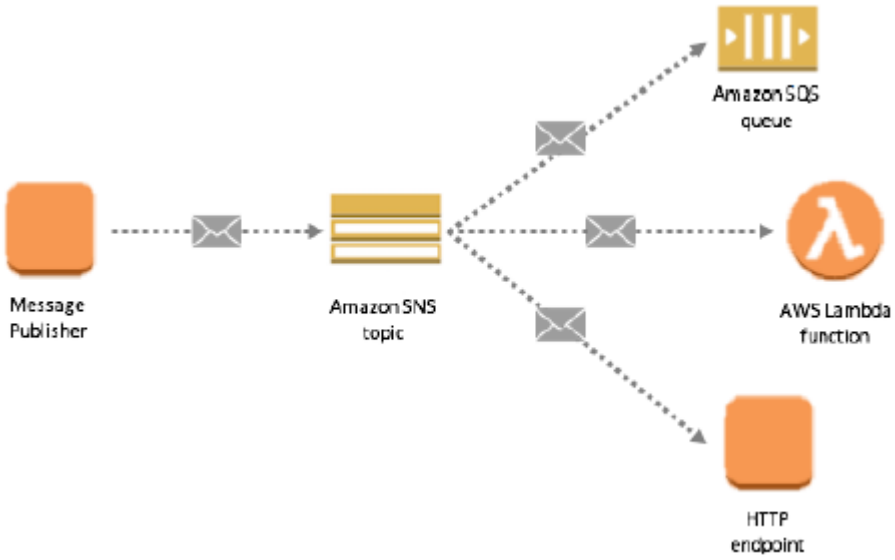
Option A is CORRECT. SNS messages can be sent to registered addresses as Email (text-based or Object) who act as subscribers to the notification

Option B is incorrect. S3 acts as a publisher of SNS notifications. When a file is uploaded to S3, it can publish an event that can then be subscribed to & acted upon

Option C is CORRECT. A lambda function can subscribe to an SNS Topic and can act on any events that are published to that Topic. An S3 PUT or CREATE event for uploading documents can have a Lambda subscriber that can pull out metadata information contained within the documents & store it in a DynamoDB database.

Option D is incorrect. CloudWatch will act as a publisher of events using alarms. Getting back to In our scenario, we can set CloudWatch alarms on the CPU utilization metrics of the EC2 instance. The alarms can then be published to an SNS Topic for notifying users.

Option E is incorrect. Dynamodb streams are events that are emitted when record modifications occur on a Dynamodb table like INSERT, UPDATE etc.They are extremely useful to create informative dashboards in real-time. Dynamodb streams can trigger a lambda function that can publish a message to an SNS Topic. So we can see here that DynamoDB stream acts as a publisher of events.



Reference:
https://docs.aws.amazon.com/sns/latest/dg/welcome.html

Q14. I have a website that hosts mission-critical applications and requires 99.999% uptime. What routing policy will I apply while using Route 53?

A. Multi Value Answer Routing
B. Failover Routing A
C. Weighted Routing
D. Simple Routing

Answer: B

Since the mission-critical applications require 99.999% uptime, I would need an Active-Active site replication of resources. Here one site's failure will result in Route 53 automatically switching to the other site, thus maintaining the uptime requirement.

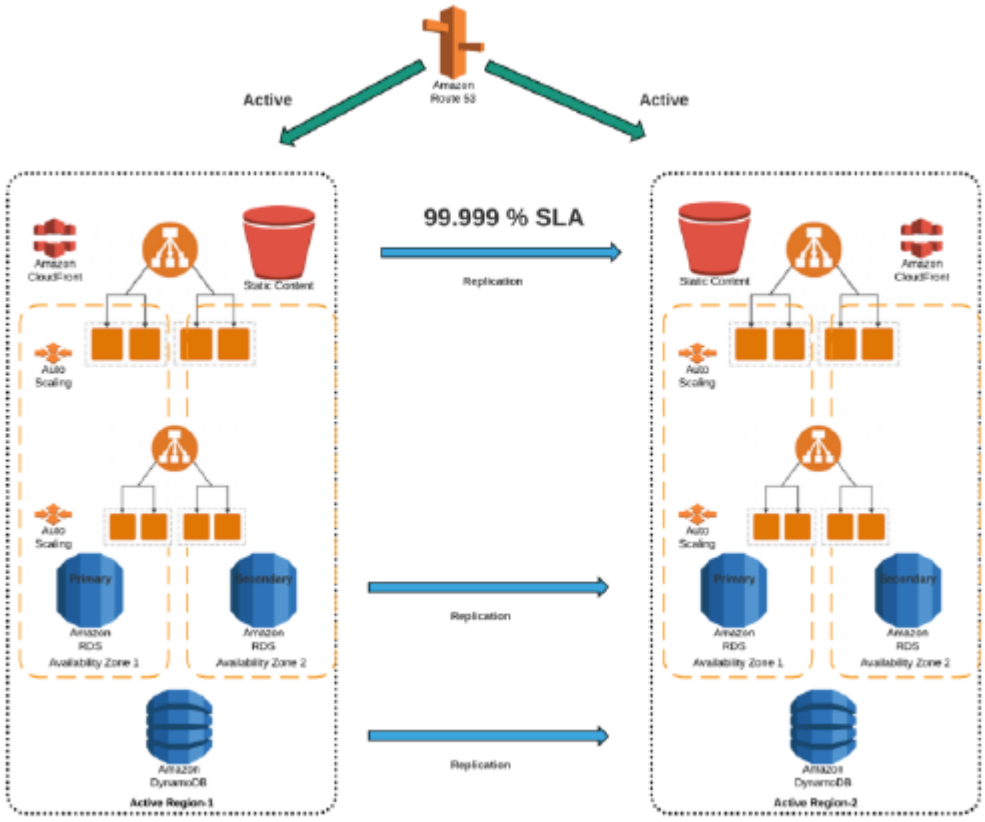
Option A is incorrect. Multivalve answer routing provides the ability to return multiple health checkable IP addresses, which is a way to use DNS to improve availability and load balancing. The critical point here is that these IP addresses may not point to servers at multiple site locations. Rather they may be servers in different availability zones within the same region. Since we add a higher level of resiliency for the critical requirement, it's always advisable to provide an entire region failure.

Option B is CORRECT. Failover routing is usually used in Disaster Recovery scenarios where an Active-Passive or Active-Active Disaster recovery configuration is required.

Option C is incorrect. A weighted routing policy is usually used to route traffic in proportions

that are specified. E.g., if there is a new version of software that needs to be tested, 20% of the traffic can be sent to that site for getting user feedback rather than sending 100% of the traffic to that site.

Option D is incorrect. A simple routing policy is used for routing traffic to a single resource, e.g., mapping an URL to a web server.



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

Q15. My containerized application requires me to define and manage capacity(CPU, Memory, Instance type) explicitly for optimizing costs while using AWS infrastructure. Which of the following technologies will I use while defining my Elastic Container Services compute instances

A. EC
B. Fargate
C. Lambda
D. Either of B or C since they are serverless technologies that are cost effective

Explanation:

Correct Answer: A

Elastic Container Services supports two launch types for deploying containers, mainly the EC2 type & the Fargate type. Fargate provides infrastructure automation for provisioning compute instances as required. Since our scenario requires explicit control of CPU & Memory resources for launching the container instances, EC2 will be the most appropriate type.

Option A is CORRECT since the user will have complete control over the VM configuration & the OS.

Option B is incorrect since Fargate automates infrastructure provisioning where a user may have limited control

Option C is incorrect since Lambda is a serverless technology & is not used within a service containerization context

Option D is incorrect since serverless technologies although may be lucrative from a cost standpoint will not have complete user control over con guring the compute instances

Diagram:

Amazon EC2	Amazon Fargate
You explicitly provision EC2 instances	The control plane asks for resources and Fargate automatically provisions
You're responsible for upgrading, patching, care of EC2 pool	Fargate provisions compute as needed
You must handle cluster optimization	Fargate handles cluster optimization
More granular control over infrastructure	Limited control, as infrastructure is automated

Q16. I require different levels of access for my application that is installed on an EC2 instance. I have configured an ENI for the same purpose. Which of the following statements is incorrect?

A. I can detach the primary ENI of my EC2 instance and connect it to another instance for moving its Elastic IP

B. I can configure a Security Group for my ENI and restrict traffic to the EC2 instance

C. I can detach a secondary ENI containing a Private IP from one EC2 instance and attach it to another

D. I can attach an Elastic IP to an EC2 instance in another subnet by releasing it from the ENI in the current subnet to which it is currently attached to

Explanation: Correct Answer: A

Option A is CORRECT. The primary ENI of an instance cannot be detached from the instance. By default, the primary ENI is created with the creation of the EC2 instance & deleted when the instance is terminated

Option B is incorrect since an EC2 instance may require restricted access to certain IP addresses. This can be achieved by creating a new ENI & attaching a Public IP & Security Group restricting permissions.

Option C is incorrect. Secondary ENI's that are created can be detached from the instance to which it is attached to & attached to another instance within the same subnet. The Private IP then gets allocated to the second instance to which it is attached currently

Option D is incorrect. ENI's are subnet specific. So for attaching an Elastic IP to an instance in a different subnet, I need to rst release it to the pool by dissociating it from an attached instance. This way, I can attach the Elastic IP to an instance in a different subnet.

Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

Q17. I need to check whether my EC2 instances are running properly. I have written a script that will help me obtain the instance's ID and then send a notification to an SNS topic. How can I obtain the instance's ID?

A. By querying the instance's Metadata
B. By querying the instances User Data
C. I need to get authorized with an IAM role prior to accessing the instance's ID using Metadata
D. I cannot use a script. I need to login to the AWS console & manually check the instance's ID & its status

Explanation: Correct Answer: A
Option A is CORRECT. An instance's Metadata provides me with information about the instance like Instance ID, Local IP, Instance Type etc..I can query the instances Meta data using an internal IP http:/ 169.254.169.254/latest/meta-data/ which can be accessed only from within an EC2 instance

Option B is incorrect. User Data is a section used for providing startup con guration to an EC2 instance. Eg if I need to have an Apache web server running on an EC2 instance after it is provisioned, I can use the User Data section & provide scripts for installing the software during instance creation

Option C is incorrect. Meta data information is available to EC2 instances by default without the need to provide an IAM role for accessing it

Option D is incorrect. Console login or manual intervention is not required to achieve this task. I can write a script & configure it to run at a scheduled time of the day wherein the EC2 instance can express itself to provide its health status.

References:
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/instancedata-data-retrieval.html

Q18. EC2 User Data provides a feature wherein I can do bootstrapping activities when the instance is created. Which of the following statements regarding User Data is incorrect?

A. AMI's created out of the EC2 instance will also run the bootstrapping commands
B. I cannot modify the User Data script once it is created
C. I need to use "sudo" in my User Data script to run as the root user
D. Both B & C A

Explanation: Correct Answer: D
Option A is incorrect. You can create an AMI out of an EC2 instance & use all its features including the User Data scripts. AMI's allow you to customize your instances during runtime & can provide e ect to any compliance policies like Updating security patches automatically that may be mandated by an Organization

Option B is incorrect. I can update the User Data script by stopping the EC2 instance through both the AWS console & the CLI.

Option C is incorrect. The script commands within User Data run as root. So I need not use sudo explicitly for running them

Option D is CORRECT since both B & C are incorrect and I need to choose only one statement in the given scenario.

References:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html

3 SECURITY & COMPLIANCE

Q1. Which of the below can be configured to enhance the security at the subnet level?

A. Virtual Private Cloud (VPC)

B. Configure transitive VPC peering

C. NACL (Network Access Control List)

D. Security Group

Answer: C

Explanation:

Option A is INCORRECT. Virtual Private Cloud (VPC) is a virtual network that lets us launch AWS resources in the denied virtual network.

Option B is INCORRECT. Configure transitive VPC peering is invalid as this is not supported in AWS.

Option C is CORRECT. NACLs can be configured to enhance the security at the subnet level.

Option D is INCORRECT. Security Group acts as a virtual firewall by controlling the traffic both inbound and outbound. Security group acts at the instance level.

Reference:
https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-con gurations.html
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
https://k21academy.com/amazon-web-services/aws-certified-solutions-architect-professional-sapc01/

Q2. Under the "**Shared Responsibility Model**," which of the listed below is Customer's Responsibility?

A. Hardware of the AWS underlying infrastructure

B. Client-side data encryption

C. Database of the AWS infrastructure

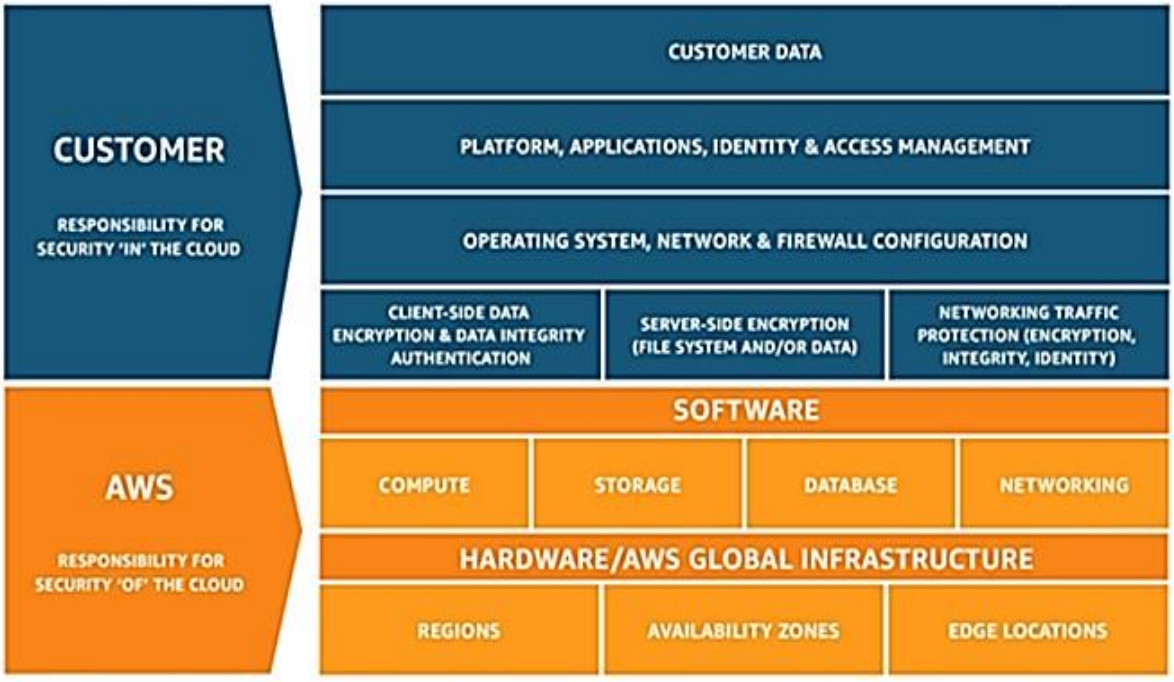
D. Networking of the AWS infrastructure

Answer: B

Explanation:

Option A is INCORRECT. Refer to the link and diagram below. Option B is CORRECT. Refer to the link and diagram below.

Option C is INCORRECT. Refer to the link and diagram below. Option D is INCORRECT. Refer to the link and diagram below.



Reference:

https://aws.amazon.com/compliance/shared-responsibility-model/

Q3. To make programmatic calls to AWS, a user was provided an access key ID and secret access key. However, the user has now forgotten the shared credentials and cannot make the required programmatic calls. How can an access key ID and secret access key be provided to the user?

A. Use the “Forgot Password” Option

B. Use “Create New Access Key” by logging in to AWS Management Console as the root user.

C. Credentials cannot be generated

D. Raise a ticket with AWS Support

Answer: B

Explanation:

Option A is INCORRECT. This is an invalid option.

Option B is CORRECT.

Option C is INCORRECT. This is an incorrect option. We can create a new access key by logging in to Management Console as a root user.

Option D is INCORRECT. This is an incorrect option. We can create a new access key by logging in to Management Console as a root user.

Reference:

https://k21academy.com/amazon-web-services/create-access-and-secret-keys-in-aws/
https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html

Q4. To enable an application on an EC2 instance to perform some actions, the developer is required to grant access to the application for a few AWS resources. The developer plans to provide his credential to the instance. However, as the developer's credentials are long-term, the developer is looking for an alternative to reduce the security risk.

What can the developer do in this scenario to enable applications on EC2 to get access to the required AWS resources temporarily?

A. Use "IAM Roles"

B. Use "IAM Group"

C. Use "IAM Tags"

D. There is no alternate way. A developer needs to give his credentials and revoke access when the required action is done.

Explanation:

Answer: A

IAM roles facilitate access delegation to services/users that in general do not have access to AWS resources of your organization. Users could assume the role (IAM Users) and/or services (AWS services) for getting temporary security credentials. This can then be used to perform the required actions.

An IAM group is a service to grant/revoke/manage permissions on a collection of IAM users. IAM tags add custom attributes to IAM users or roles. IAM tags use key-value pairs.

Option A is CORRECT as the IAM role can enable applications on EC2 to get access to the required AWS resources temporarily.

Option B is INCORRECT because the IAM group is a collection of IAM Users and helps in access management.

Option C is INCORRECT because IAM tags are simply "labels" that add custom attributes to the users/roles.

Option D is INCORRECT because we can use IAM Roles in the scenario.

Reference:

https://k21academy.com/amazon-web-services/aws-solutions-architect/aws-identity-and-accessmanagement-iam/

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

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

Q5. An application requires access to a database to retrieve certain information and this action would require the developer to hard code the credentials. Hard coding the credentials are not a best practice. He can securely store encrypted credentials and retrieve them when required, eliminating the need of hard-coding credentials in the application. Which AWS service would you suggest to the developer?

A. AWS Secrets Manager

B. AWS Encryption SDK

C. AWS Security Hub

D. AWS Artifact

Explanation:

Answer: A

AWS Secrets Manager helps in securely storing encrypted credentials and ensures retrieval when required. The use of AWS Secrets Manager eliminates the need for hard-coding credentials in the application.

AWS Encryption SDK is the encryption library that makes client-side encryption best-practice easier. The encryption libraries facilitate cryptographic services and do not require AWS or any AWS service.

AWS Security Hub gives you a comprehensive view of your high-priority security alerts and security posture across your AWS accounts.

AWS Artifact is a central resource for all the information pertaining to compliance. AWS artifact provides on-demand access to compliance reports at no additional cost.

Option A is CORRECT as AWS secrets Manager is an easy way to store encrypted credentials and perform on-demand retrieval safely.

Option B is INCORRECT because AWS Encryption SDK does not facilitate storing and retrieving the credentials but makes implementation of the client-side encryption best practices easier.

Option C is INCORRECT because AWS Security Hub facilitates the view of high-priority security alerts and provides a view of the security landscape across AWS accounts.

Option D is INCORRECT as AWS artifacts does not help with the credentials storing and retrieval, but facilitates information pertaining to compliance centrally.

Reference:

https://docs.aws.amazon.com/secretsmanager/

https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/introduction.html

https://aws.amazon.com/security-hub/

https://docs.aws.amazon.com/artifact/

Q6. When provisioning a security certificate from AWS Certificate Manager (ACM), which of the following statements is true? Choose TWO.

A. ACM-issued security certificate cannot be applied to an application load balancer.

B. To verify a security certificate, a CNAME record would need to be created.

C. Third-party security certificates cannot be applied to AWS resources.

D. To verify a security certificate, the administrator would need to acknowledge a verification email sent to an address of their choice.

E. A security certificate issued in ACM can only be applied to one AWS resource.

Explanation:

Correct Answer: B, D

There are two ways to validate and verify the issuance of a security certificate in AWS Certificate Manager. These are creating a CNAME record in the hosted zone of the domain or email confirmation sent to the requester's email address.

Option A is INCORRECT because it is possible to apply ACM-issued security certificates on the Application load balancer.

Option C is INCORRECT because AWS customers can upload third-party security certificates into ACM and manage and apply them to AWS resources.

Option E is INCORRECT because security certificates issued in ACM can be applied to multiple AWS resources.

Reference:

https://k21academy.com/amazon-web-services/aws-certificate-manager-acm/

https://docs.aws.amazon.com/acm/latest/userguide/gs-acm-validate-dns.html

https://docs.aws.amazon.com/acm/latest/userguide/gs-acm-validate-email.html

Q7. An administrator would like VPCs in three different AWS accounts to access on-premises resources via a VPN connection terminating on a Transit Gateway. Each of the VPCs is in distinct AWS regions. How can this be achieved?

A. Use AWS Resource Access Manager (RAM) to share the Transit Gateway resource.

B. Configure a Virtual Private Gateway (VGW) for each VPC and then extend the VPN tunnels to them.

C. Create VPC attachments from each of the VPCs to the Transit Gateway.

D. Configure VPC peering connections between the VPCs and then route traffic from on premises through the VPN to the Transit Gateway and then to each VPC peer.

Explanation:

Correct Answer: A

AWS Resource Access Manager (AWS RAM) allows AWS customers to share resources between multiple AWS accounts. In this scenario, it is possible to share the access to the Transit Gateway resource with the three AWS accounts, even if the VPCs are in distinct AWS regions.

Option B is INCORRECT because it is not possible to extend the VPN tunnels. In the scenario, the VPN tunnels terminate on the Transit Gateway in one of the AWS accounts.

Option C is INCORRECT because it cannot create VPC attachments without sharing the Transit Gateway resource.

Option D is INCORRECT because it has transitive routing connotations. This is not permissible in the AWS environment.

Reference:

https://docs.aws.amazon.com/ram/latest/userguide/what-is.html

Q8. An administrator receives an alert and detailed report regarding credit card information that has been erroneously uploaded by a user into one of the S3 buckets during an online questionnaire exercise for a survey. Which AWS service provided this detection and report?

A. Amazon Inspector
B. Amazon Event Bridge
C. Amazon Detective
D. Amazon Macie

Explanation:

Correct Answer: D

Amazon Macie is a fully managed AWS service that provides data security and privacy using machine learning algorithms, artificial intelligence and pattern matching. These mechanisms detect, discover, monitor, report and protect sensitive data stored in Amazon Simple Storage Service (Amazon S3). Macie can detect and alert sensitive data, such as bank credit card information.

Option A is INCORRECT because Amazon Inspector does not assess actual data stored in S3. It primarily assesses applications for exposure and vulnerability.

Option B is INCORRECT because Amazon EventBridge does not perform the function of detecting sensitive data.

Option C is INCORRECT because primarily relevant in establishing the root cause of security incidences or suspicious activities within the AWS environment.

Reference:

https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html

Q9. During an audit process, an organization is advised by the audit committee to centrally manage all the VPC security groups and WAF rules across their AWS environment. Given that the organization has multiple AWS accounts, how can this be achieved?

A. AWS Identity & Access Management (IAM)

B. AWS Firewall Manager

C. Amazon Cloud Directory

D. AWS Security Hub

Correct Answer: B

AWS Firewall Manager makes it possible to manage VPC security groups, AWS Shield Advanced and WAF rules on one platform even across multiple AWS accounts.
Option A is INCORRECT because AWS Identity & Access Management (IAM) does not allow for the management of VPC security groups or WAF rules.

Option C is INCORRECT because Amazon Cloud Directory is a repository for developer objects. The service does not have the functionality to centrally manage all the VPC security groups or WAF rules in the AWS environment.

Option D is INCORRECT because AWS Security Hub is a full-view, single-look, comprehensive depiction of the security state of the customer's AWS environment. The service collates security data across AWS accounts and facilitates the analysis of data security patterns. It identifies the highest priority security areas in the customer's AWS environment.

Reference:

https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html

Q10. Which of the following statements accurately describe a function of AWS Secrets Manager? [Select Two]

A. Encrypts authentication information in code, ensuring that it is unreadable, that is, not in plain text.

B. Replaces the need to hardcode authentication credentials in code.

C. Makes it possible to include an API call in code that retrieves authentication information from a central repository.

D. Automatically rotates and updates the code in the application build, ensuring that repositories are kept up to date.

E. Facilitates the embedding of authentication information in code during runtime.

Correct Answer: B, C

AWS Secrets Manager allows users to replace authentication information in code with an API call to Secrets Manager. This API call then retrieves the secret programmatically. This safeguards the secret from being compromised since the secret is removed from the code. AWS Secrets Manager automatically rotates the secret in accordance with specified schedules which allows the implementation of more secure short-term secrets. These, in turn, reduce the risk of authentication information in code being compromised.

Option A is INCORRECT because AWS Secrets Manager does not encrypt authentication information whilst it is in the code.

Option D is INCORRECT because AWS Secrets Manager does not automatically rotate or update the application code. Rather, it automatically rotates the secret in accordance with specified schedules.

Option E is INCORRECT because AWS Secrets Manager does not facilitate embedding authentication information in code during runtime. Developers do not need to hard-code authentication information in code.

Reference:

https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

Q11. A client has decided to go for a MySQL RDS database on the AWS cloud based on its Scalability & High Availability features. When he does so, what role does he play in making the database secure? (Select TWO.)

A. He can restrict RDS access to the database by using a Security Group.

B. He can provide the most recent updates of his database software installed on the EC2 Instance for preventing Security attacks.

C. He can provide the most recent versions of his Operating System on the EC2 instance for preventing Security attacks.

D. He can Encrypt database data at rest by using EBS volume storage encryption.

E. He can plan for backup & recovery strategies for data that may be lost.

Explanation:

Answers: A and E

RDS is a managed service (Database as a Service) that allows the user to ease administrative tasks like Database software updates and Operating System patch updates. Thus, it helps the user concentrate more on the design/development of the database. The instance class types (EC2 VM's) that support the database instance configuration are abstracted from the user since it is provided as a service. All in all, RDS offers automatic DB installation process, storage disk provisioning, Database upgrades, Security patches and backups of SQL Server databases. In this scenario, we would like to know the tasks that a user can perform as a part of the Shared responsibility model for security in an RDS database.

Option A is CORRECT. Security Groups can be used to control Ingress / Egress traffic owing in & out of an RDS database instance. A user can configure an Ingress security group rule for restricting traffic to certain IP addresses of an RDS port such as 3306.

Option B is incorrect. Database instances are abstracted from the user & database software updates are managed by the service provider (AWS).

Option C is incorrect. Since the instance types are abstracted from the user, the OS security patches are also controlled by the service provider (AWS).

Option D is incorrect. Data encryption at rest is possible in an RDS instance. However, using an EBS volume will not be possible since that will require much more control to the instance hosting the Database to mount an EBS volume. RDS automatically manages storage disk provisioning. It allows a user to select the storage type during database creation/modification time from the following types: General purpose SSD, Provisioned IOPS, Magnetic.

Option E is CORRECT. Although RDS provides an automated backup facility, the user needs to enable it & plan for the window time where the backup process can be initiated. RDS also provides the user with a facility to do manual backups (Point in time DB snapshots) which can be planned.

References:

https://aws.amazon.com/blogs/database/common-administrator-responsibilities-on-amazon- rds-and-aurora-for-postgresql-databases/

Q12. I have a Mobile App that needs to access AWS resources like S3, DynamoDB. What is the best way to allow users of the mobile app access to these AWS resources?

A. Keep the Security Credentials associated with the AWS resource access within the Mobile App

B. Use Security Token Service (STS) with Identity Federation that will allow a user access to resources within a session

C. Create Users & Groups within IAM and assign IAM policies for accessing the resources

D. Have the mobile app connect to another web application running on an EC2 instance that can assume a role for accessing the AWS resources

Explanation:

Answer: B

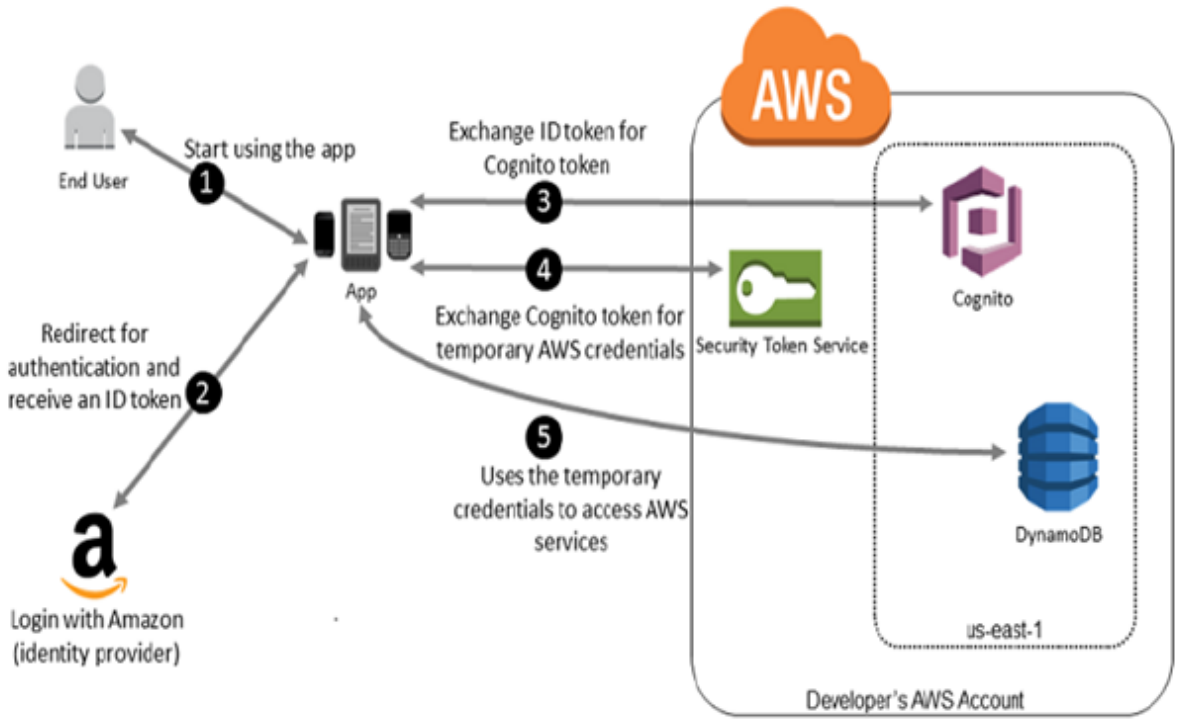
A mobile app that becomes popular can have a large user base. The best way to provide access to AWS resources in this scenario will be to use Federated Identity access using External Identity Providers (IdP) like Amazon, Facebook, Google etc. The mobile app can establish trust with these well-known IdPs and take advantage of the authentication mechanisms to validate user identity. As shown in the figure below, the mobile app uses Amazon as the external IdP for accepting user credentials & authenticating him. Using Cognito & the Security Token Service, the Mobile App then gets temporary Security Credentials for accessing the AWS resources required by the app. The role associated with the STS token and its assigned policies determine what can be accessed.

Option A is incorrect. Distributing long-term AWS Security Credentials with external applications is not recommended since the credentials may be compromised resulting in security breaches.

Option B is CORRECT. The STS token will contain temporary credentials with a Role indicating the access level that a mobile app user can have. The security credentials will be valid for a specific user session only.

Option C is incorrect. Creating an ever-growing set of Users within AWS IAM and assigning them permissions for accessing AWS resources will be impractical.

Option D is incorrect. Although it is a viable option to connect to an EC2 instance running a similar web application, it will duplicate e ort on the developer's part.



References:

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

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

Q13. I have a compliance requirement for my application, stating that unrestricted SSH access to any EC2 instance needs to be immediately notified to an admin. Which services can I use to achieve the requirement?

A. AWS Trusted Advisor, Amazon SNS

B. AWS Inspector, Amazon SNS

C. AWS Config, Amazon SNS

D. Both B & C

Explanation:

Answer: D

Both AWS Inspector & AWS Config can scan EC2 instances, access their network exposure, and then integrate with Amazon SNS to send notifications. Trusted Advisor also can check for overly permissive access of EC2 instances. Still, the notifications can be performed by monitoring the Trusted Advisor check results with AWS CloudWatch events that can use specific targets like Lambda, SNS etc.

Option A is incorrect. Trusted Advisor results cannot be directly configured with SNS. They need to be monitored using CloudWatch events.

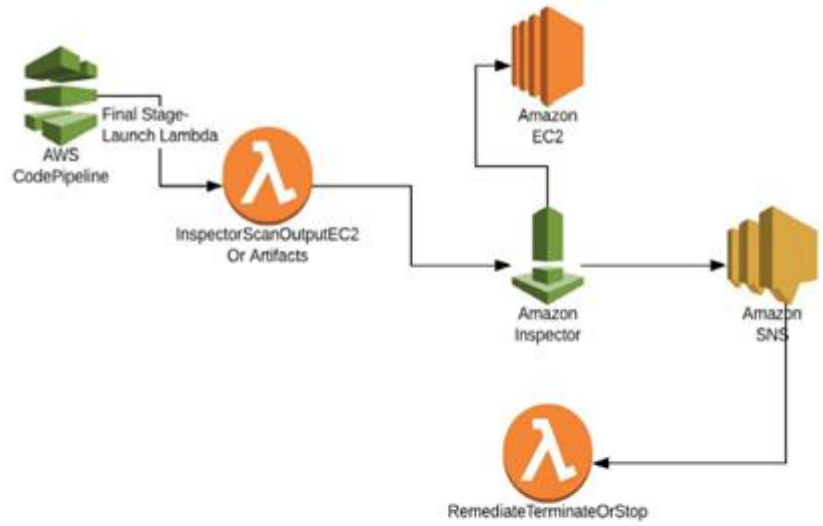
Option B is incorrect. For the given scenario, both AWS Con g & AWS Inspector can be configured to send notifications to SNS when a compliance breach is observed.

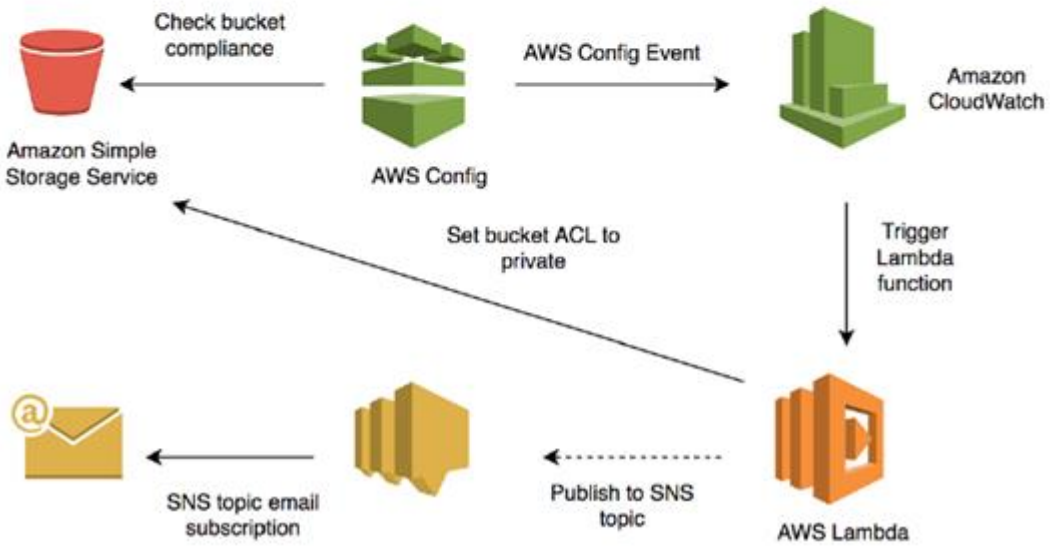
Option C is incorrect. The same explanation is given in Option B.

Option D is CORRECT. The Network Reachability rules package recently released for AWS Inspector helps analyze Amazon VPC network configuration to determine whether an EC2 instance can be reached from external networks like the Internet. It does it by analyzing network configurations like Security Groups, NACL's, Route tables etc. The assessment that is run, its security endings can be published to an SNS topic.

AWS Config's Configuration Streams can be configured with resources like Amazon SNS. Within AWS Config, you can configure Managed rules or Custom rules that can detect compliance violations & use the configuration stream for sending notifications.

Diagrams:





References:

https://aws.amazon.com/blogs/security/amazon-inspector-assess-network-exposure-e 2-instances-aws network-reachability-assessments/

https://aws.amazon.com/blogs/security/how-to-remediate-amazon-inspector-security-ndings-automatically/

https://aws.amazon.com/blogs/aws/trusted-advisor-console-basic/

https://docs.aws.amazon.com/awssupport/latest/user/cloudwatch-events-ta.html

4 BILLING & PRICING

Q1. An organization has started a new project to create memes based on user comments and uploaded images. As this new project is started on a pilot basis and is not pursued rigorously, cost efficiency is emphasized and not the uptime and processing time. Given these priorities, which EC2 Instance should be preferred?

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

Explanation:
Answer: B
Option A is INCORRECT. On-Demand Instances are costlier than spot instances.

Option B is CORRECT. Spot instances are the most cost-efficient option. Please note interruptions are stated to be not an issue.

Option C is INCORRECT. Dedicated Instances are instances that are dedicated to a single user. Dedicated instances are not suitable for these types of scenarios.

Option D is INCORRECT. Scheduled Reserved Instances will not be preferable over spot instances in this scenario because interruptions are stated to be not an issue. Nothing in this scenario states long-term requirements. Scheduled Reserved Instances require long term commitment.

Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html

Q2. An organization has developed an application that creates event-based memes. The organization has decided to run this application uninterruptedly for the period of a planned sporting event so that the fans of teams can create memes and share them on social media to show their support. The sporting event is 3 months long. Which EC2 instance will be best suited for this scenario?

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

Explanation:
Answer: A

The point to be noted in this scenario is

-Application is to be run uninterruptedly.

-Duration of the requirement is 3 months.

As the duration is 3 months, Option B and Option D are not a good choice.

Since the application needs to run uninterruptedly, Option C is not a good choice as there is the probability of interruptions in spot instances.

Option A is CORRECT. Option B is INCORRECT. Option C is INCORRECT. Option D is INCORRECT.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html

Q3. Which of the below statements is correct regarding the AWS trusted advisor checks available to AWS Basic Support customers and AWS Developer Support customers?

A. AWS Basic Support customers and AWS Developer Support customers both get access to 6 security checks and 50 service limit checks.
B. AWS Basic Support customers get access to 6 security checks along with 50 service limit checks and AWS Developer Support customers gets access to all 115 Trusted Advisor checks
C. AWS Basic Support customers and AWS Developer Support customers both get access to all 115 Trusted Advisor checks D. None of the above is true

Explanation:
Answer: A

Option A is CORRECT. This statement is correct. Both the basic support and developer support customers get access to 6 security checks and 50 service limit checks.

Option B is INCORRECT. Option A is correct. AWS Enterprise and Business support customers get access to all the trusted advisor checks.

Option C is INCORRECT. Option A is correct. AWS Enterprise and Business support customers get access to all the trusted advisor checks.

Option D is INCORRECT.

Reference:
https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

Q4. Which S3 storage class is preferable for storing on-prem data backup (Secondary backup) copy?

A. S3 Standard
B. S3 Standard-Infrequent Access
C. S3 Intelligent-Tiering
D. S3 One Zone-Infrequent Access

Explanation:
Answer: D

S3 One Zone-Infrequent Access should be the preferable S3 storage class as other storage classes are costly options. In this scenario, the data is a secondary backup copy and hence shall

be accessed infrequently. Data resilience is not mandatorily required since the data is a secondary backup copy.
Option A is INCORRECT. S3 Standard will not be preferred as this will be a costly option when the requirement could be fulfilled using S3 One Zone IA.

Option B is INCORRECT. S3 Standard-Infrequent Access will not be preferred as this will be a costly option when the requirement could be fulfilled by using S3 One Zone IA.

Option C is INCORRECT. S3 Intelligent-Tiering is incorrect. Because this is apt for data with changing patterns and here the pattern is not changing. This is also a costly option.

Option D is CORRECT.

Reference:
https://k21academy.com/amazon-web-services/aws-solutions-architect/aws-storage-overviewtypes-benefits/
https://aws.amazon.com/s3/storage-classes/
https://aws.amazon.com/about-aws/whats-new/2018/04/announcing-s3-one-zone-infrequentaccess-a-new-amazon-s3-storage-class/

Q5. Which of the below listed AWS service(s) and feature(s) are free of cost?

A. Amazon Cloud Directory
B. Amazon Macie
C. Amazon Guard Duty
D. IAM

Explanation:
Answer: D
Option A is INCORRECT because Amazon Cloud Directory follows the “Pay what you use” model.

Option B is INCORRECT because Amazon Macie is not a free service. Option C is INCORRECT because Amazon Guard Duty is not a free service. Option D is CORRECT because IAM is offered by AWS free of cost.

Reference:
https://k21academy.com/amazon-web-services/aws-solutions-architect/aws-identity-and-accessmanagement-iam/
https://aws.amazon.com/macie/pricing/?p=ps
https://aws.amazon.com/guardduty/pricing/?p=ps https://aws.amazon.com/iam/

Q6. I make a conscious decision to move my on-premises workloads to AWS cloud. What are the steps that I need to take so that my costs are not mismanaged? **(Select TWO.)**

A. Stopping my EC2 instance when not needed is the best practice to eliminate any billing associated with it.
B. I should not allocate Elastic IP addresses with a running instance due to charges they will incur.
C. Spot instances will be useful for my dev/test environment workloads.
D. Use EBS lifecycle policies to delete old EBS snapshots.
E. Use Amazon CloudWatch Logs to monitor the application exceptions.

Explanation:
Answers: C and D

Option A is incorrect. Although stopping an EC2 instance will ensure that you will no longer be charged for the instance, any attached EBS volumes will continue to remain in the availability zone & standard charges for the EBS volume will continue to be applied to them. So, the best practice will be to terminate the EC2 instance when not needed. That will result in detachment & deletion of any EBS volumes ensuring that there is no billing happening for the VM provisioned and their attached storage.

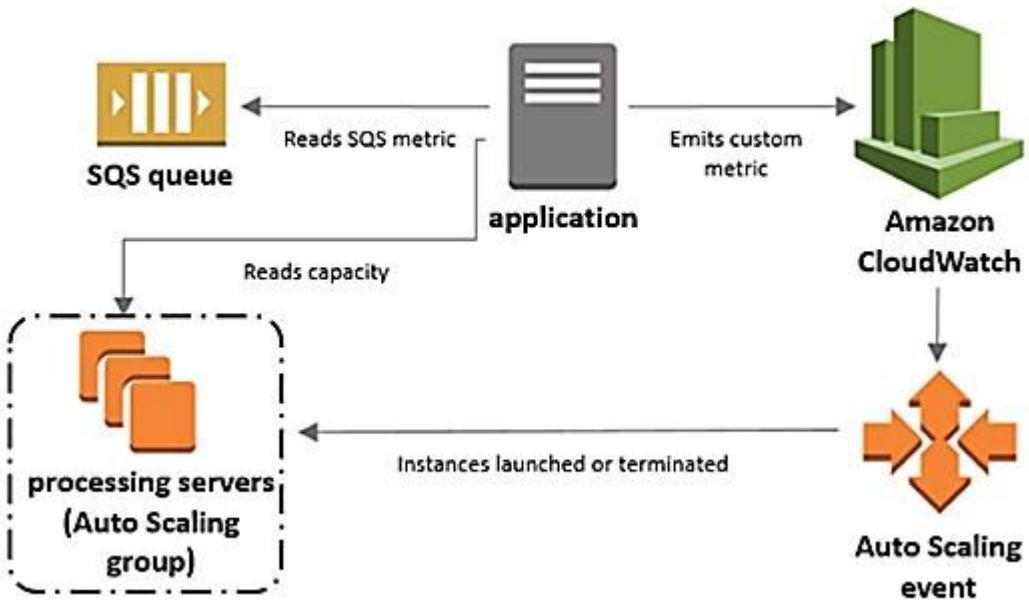
Option B is incorrect. On the contrary, Elastic IP(EIP) should always be associated with a running instance that comes without a charge. Releasing EIP's after stopping the instance or when they are not associated with the instance becomes necessary for avoiding charges.

Option C is CORRECT. Dev/Test environments will not have mission-critical applications running within them. So, it will be an excellent idea to use Spot instances for those environments, which will bring in cost efficiency.

Option D is CORRECT. This option can delete old and unused EBS snapshots to reduce the costs.

Option E is incorrect. CloudWatch Log monitoring helps in incident detection & resolution rather than providing cost benefits.

Diagrams:



References:
https://k21academy.com/amazon-web-services/aws-solutions-architect/aws-storage-overviewtypes-benefits/
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

FREE CLASS

Register for our FREE Class To know about What is AWS Solution Architect role, most important AWS services you will master Like - Why & Who Should Learn AWS?, Cloud Service, Deployment Models, and AWS Services, Demo: Creating S3 Bucket & Make a Data available to the Entire world, IAM, Compute, Storage, Networking, HA & DR Architecture and what to study Including Hands-On labs you must perform to clear [AWS SAA-C02] Amazon AWS Solution Architect Certification, so that you can stay ahead in your career and earn a lot more
https://k21academy.com/awssa02

K21Academy
Learn Cloud from Experts

amazon web services

ABOUT AUTHOR

Atul Kumar Is An Oracle ACE, Author & Oracle Certified Cloud Architect With 21+ Years of IT Experience. Helped 8000+ Individuals to learn cloud including Azure, Oracle, Google AWS Cloud.

He is helping his customer to become an expert in AWS Certified Cloud Practitioner

/oracleappsdba

/k21academy

/k21academy

/k21academy

/k21academy

K21Academy
Learn Cloud from Experts

amazon web services

K21Academy
Learn Cloud from Experts

contact@k21academy.com

FREE CLASS: https://k21academy.com/awssa02