May 5 SET A -CH5

Total points 58/65

Time: 120 minutes
Full Marks : 65
Pass Marks: 47

Email *

07yamini2055@gmail.com

0 of 0 points

Full Name *

Ira Chand

All Questions are compulsory

58 of 65 points

✗ According to the AWS Shared Responsibility Model, which of the following are responsibilities of AWS? (Select two) *0/1

- [ ] Maintaining Amazon S3 data in different availability zones to keep it durable
- [ ] Creating S3 bucket policies for appropriate user access
- [x] Enabling Multi Factor Authentication on AWS accounts in your organization ✗
- [x] Creating IAM role for accessing Amazon EC2 instances ✗
- [ ] Replacing faulty hardware of Amazon EC2 instances

Correct answer

- [x] Maintaining Amazon S3 data in different availability zones to keep it durable
- [x] Replacing faulty hardware of Amazon EC2 instances

✓ Which AWS service is an object-based serverless storage system that is able to handle a nearly unlimited amount of data? *1/1

- ○ Amazon DynamoDB
- ○ Amazon EC2
- ◉ Amazon S3 ✓
- ○ Amazon ECS

Feedback

Amazon S3 is an object-based serverless storage system that is able to handle a nearly unlimited amount of data.

✓ A company needs to keep sensitive data in its own data center due to compliance but would still like to deploy resources using AWS. Which Cloud deployment model does this refer to? *1/1

- ○ Private Cloud
- ○ On-premises
- ○ Public Cloud
- ◉ Hybrid Cloud ✓

Feedback

Explanation
Correct option:

Hybrid Cloud

A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud. The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend, and grow, an organization's infrastructure into the cloud while connecting cloud resources to the internal system.

Overview of Cloud Computing Deployment Models: via - https://aws.amazon.com/types-of-cloud-computing/

Incorrect options:

Public Cloud - A public cloud-based application is fully deployed in the cloud and all parts of the application run in the cloud. Applications in the cloud have either been created in the cloud or have been migrated from an existing infrastructure to take advantage of the benefits of cloud computing.

Private Cloud - Unlike a Public cloud, a Private cloud enables businesses to avail IT services that are provisioned and customized according to their precise needs. The business can further avail the IT services securely and reliably over a private IT infrastructure.

On-premises - This is not a cloud deployment model. When an enterprise opts for on-premises, it needs to create, upgrade, and scale the on-premise IT infrastructure by investing in sophisticated hardware, compatible software, and robust services. Also, the business needs to deploy dedicated IT staff to upkeep, scale, and manage the on-premise infrastructure continuously.

Reference:

https://docs.aws.amazon.com/whitepapers/latest/public-sector-cloud-transformation/selecting-the-right-cloud-for-workloads-differences-between-public-private-and-hybrid.html

✓ Which AWS service can be used to prepare and load data for analytics using an extract, transform and load (ETL) process? *1/1

- ○ AWS Lambda
- ○ Amazon Athena
- ◉ AWS Glue ✓
- ○ Amazon EMR

Feedback

Explanation
AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.

You can point AWS Glue to data stored on AWS, and AWS Glue discovers the data and stores the associated metadata (e.g. table definition and schema) in the AWS Glue Data Catalog. Once cataloged, the data is immediately searchable, queryable, and available for ETL.

CORRECT: "AWS Glue" is the correct answer.

INCORRECT: "AWS Lambda" is incorrect. AWS Lambda is a serverless application that runs code as functions in response to events

INCORRECT: "Amazon EMR" is incorrect. Amazon Elastic Map Reduce (EMR) provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances

INCORRECT: "Amazon Athena" is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.

References:

https://aws.amazon.com/glue/

✓ A company is planning to run a global marketing application in the AWS Cloud. The application will feature videos that can be viewed by users. The company must ensure that all users can view these videos with low latency. Which AWS service should the company use to meet this requirement? *1/1

- ○ AWS Auto Scaling
- ○ Amazon Kinesis Video Streams
- ○ Elastic Load Balancing
- ◉ Amazon CloudFront ✓

Feedback

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

✗ A team manager needs data about the changes that have taken place for AWS resources in his account during the past two weeks. Which AWS service can help get this data? *0/1

- ○ Amazon CloudWatch
- ○ AWS Config
- ◉ AWS CloudTrail ✗
- ○ Amazon Inspector

Correct answer

- ◉ AWS Config

Feedback

Explanation
Correct option:

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

While AWS Config helps you answer questions like - "What did my AWS resource look like?" at a point in time. You can use AWS CloudTrail to answer "Who made an API call to modify this resource?"

Diagrammatic representation of how AWS Config works: via - https://aws.amazon.com/config/

Incorrect options:

Amazon CloudWatch - You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly. CloudWatch cannot however tell if the configuration of the resource has changed and what exactly changed.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security

state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of the development and IT operations.

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

Reference:

https://aws.amazon.com/config/

✓ By default, which of the following events are logged by AWS CloudTrail? * 1/1

(This question is taken from restart knowledge check)

- ○ AWS CloudTrail Insights events
- ○ Data events and Insights events
- ○ Data events
- ◉ Management events ✓

Feedback

Explanation
Correct option:

Management events

An event in AWS CloudTrail is the record of activity in an AWS account. This activity can be an action taken by a user, role, or service that is monitorable by CloudTrail. CloudTrail events provide a history of both API and non-API account activity made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

There are three types of events that can be logged in CloudTrail: management events, data events, and AWS CloudTrail Insights events.

By default, AWS CloudTrail logs all management events and does not include data events or Insights events. Additional charges apply for data and Insights events. All event types use the same CloudTrail JSON log format.

Management events provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations. Examples include registering devices, configuring rules for routing data, setting up logging etc.

Incorrect options:

Data events - Data events provide information about the resource operations performed on or in a resource. These are also known as data plane operations. Data events are often high-volume activities. The following data types are recorded: Amazon S3 object-level API activity, AWS Lambda function execution activity, Amazon S3 object-level API activity on AWS Outposts.

Data events are not logged by default when you create a trail. To record AWS CloudTrail data events, you must explicitly add to a trail the supported resources or resource types for which you want to collect activity. Additional charges apply for logging data events.

AWS CloudTrail Insights events - AWS CloudTrail Insights events capture unusual activity in your AWS account. If you have Insights events enabled, and CloudTrail detects unusual activity, Insights events are logged to a different folder or prefix in the destination S3 bucket for your trail. You can also see the type of insight and the incident time period when you view Insights events on the CloudTrail console.

Insights events are disabled by default when you create a trail. To record AWS CloudTrail Insights events, you must explicitly enable Insights event collection on a new or existing trail. Additional charges apply for logging CloudTrail Insights events.

Data events and Insights events - As mentioned above, this option is incorrect.

Reference:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-events

✓ Which AWS feature of Amazon EC2 allows an administrator to create a standardized image that can be used for launching new instances? *1/1

- (●) Amazon Machine Image ✓
- ( ) Amazon Golden Image
- ( ) Amazon EBS Mount Point
- ( ) Amazon Block Template

Feedback

An Amazon Machine Image (AMI) provides the information required to launch an instance. You can use an AMI to launch identical instances from a standard template. This is also known as a Golden Image (though no such feature exists in AWS with this name). An AMI is created from an EBS snapshot and also includes launch permissions and a block device mapping.

CORRECT: "Amazon Machine Image" is the correct answer.

INCORRECT: "Amazon Golden Image" is incorrect as this is not an AWS feature.

INCORRECT: "Amazon Block Template" is incorrect. Amazon Block Templates do not exist.

INCORRECT: "Amazon EBS Mount Point" is incorrect. An Amazon EBS Mount Point is not an AWS feature. You do mount EBS volumes however this is within the operating system. Block device mappings are used in AMIs to specify how to mount the EBS volume.

References:

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

✗ AWS are able to continue to reduce their pricing due to: * 0/1

- (●) Pay-as-you go pricing ✗
- ( ) The AWS global infrastructure
- ( ) Reserved instance pricing
- ( ) Economies of scale

Correct answer

- (●) Economies of scale

Feedback

Explanation
By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay as-you-go prices.

CORRECT: "Economies of scale" is the correct answer.

INCORRECT: "The AWS global infrastructure" is incorrect. The global infrastructure is the basis of the AWS platform but it is not the reason prices continue to reduce.

INCORRECT: "Pay-as-you go pricing" is incorrect. This pricing model is a benefit but not the reason unit prices are reducing.

INCORRECT: "Reserved instance pricing" is incorrect. This pricing model results in savings for customers in specific areas but not the reason for the overall reduction in prices.

References:

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

✓ Which of the following are the advantages of using the AWS Cloud? (Select TWO) *1/1

- [x] Stop guessing about capacity ✓
- [ ] Limited scaling
- [ ] Trade operational expense for capital expense
- [ ] AWS is responsible for security in the cloud
- [x] Increase speed and agility ✓

Feedback

Explanation
Correct options:

Increase speed and agility

Stop guessing about capacity

Exam Alert:

Please check out the following six advantages of Cloud Computing. You would certainly be asked questions on the advantages of Cloud Computing compared to a traditional on-premises setup:

via - https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

Incorrect options:

Limited scaling - Scaling is not limited in the cloud. You can access as much or as little capacity as you need, and scale up and down as required with only a few minutes' notice.

AWS is responsible for security in the cloud - AWS is responsible for the security OF the cloud, which means AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

Trade operational expense for capital expense - In the cloud, you trade capital expense (CAPEX) for the operational expense (OPEX). Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can pay only when you consume computing resources, and pay only for how much you consume.

Reference:

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

✓ Which of the following statements is an AWS best practice when architecting for the Cloud? *1/1

- ○ Servers, not services
- ◉ Automation ✓
- ○ Close coupling
- ○ Security comes last

Feedback

Explanation
Correct option:

Automation

Automation should be implemented to improve both your system's stability and the efficiency of your organization. There are many services to automate application architecture (AWS Elastic Beanstalk, Auto Scaling, AWS Lambda, etc.) to ensure more resiliency, scalability, and performance.

Incorrect options:

Servers, not services - The correct best practice is: "Services, not servers". AWS recommends developing, managing, and operating applications, especially at scale, using the broad set of compute, storage, database, analytics, applications, and deployment services offered by AWS to move faster and lower IT costs.

Close coupling - The correct best practice is: "Loose coupling". AWS recommends that, as application complexity increases, IT systems should be designed in a way that reduces interdependencies. Therefore, a change or a failure in one component should not cascade to other components.

Security comes last - AWS allows you to improve your security in many, more simple ways. Therefore, you should take advantage of this and implement a high level of security.

Reference:

https://aws.amazon.com/architecture/well-architected/

✓ Adding more CPU/RAM to an Amazon Elastic Compute Cloud (Amazon EC2) instance represents which of the following? *1/1

- ○ Managing increasing volumes of data
- ○ Loose coupling
- ◉ Vertical scaling ✓
- ○ Horizontal scaling

Feedback

Explanation
Correct option:

Vertical scaling

A vertically scalable system is constrained to running its processes on only one computer; in such systems, the only way to increase performance is to add more resources into one computer in the form of faster (or more) CPUs, memory, or storage.

Incorrect options:

Horizontal scaling - A horizontally scalable system is one that can increase capacity by adding more computers to the system.

Managing increasing volumes of data - Traditional data storage and analytics tools can no longer provide the agility and flexibility required to deliver relevant business insights. That's why many organizations are shifting to a data lake architecture. A data lake is an architectural approach that allows you to store massive amounts of data in a central location so that it's readily available to be categorized, processed, analyzed, and consumed by diverse groups within your organization.

Loose coupling - As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components. This means that IT systems should be designed in a way that reduces interdependencies—a change or a failure in one component should not cascade to other components.

Reference:

https://wa.aws.amazon.com/wat.concept.horizontal-scaling.en.html

✗ A media company uses Amazon Simple Storage Service (Amazon S3) for storing all its data. Which storage class should it consider for cost-optimal storage of the data that has random access patterns? *0/1

- ○ Amazon S3 Random Access (S3 Random-Access)
- ◉ Amazon S3 Standard-Infrequent Access (S3 Standard-IA) ✗
- ○ Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)
- ○ Amazon S3 Standard (S3 Standard)

Correct answer

- ◉ Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

Feedback

Explanation
Correct option:

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is the only cloud storage class that delivers automatic cost savings by moving objects between four access tiers when access patterns change. The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without operational overhead. It works by storing objects in four access tiers: two low latency access tiers optimized for frequent and infrequent access, and two optional archive access tiers designed for asynchronous access that are optimized for rare access.

Amazon S3 Intelligent-Tiering works by storing objects in four access tiers: two low latency access tiers optimized for frequent and infrequent access, and two opt-in archive access tiers designed for asynchronous access that are optimized for rare access. Objects uploaded or transitioned to S3 Intelligent-Tiering are automatically stored in the Frequent Access tier. S3 Intelligent-Tiering works by monitoring access patterns and then moving the objects that have not been accessed in 30 consecutive days to the Infrequent Access tier. Once you have activated one or both of the archive access tiers, Amazon S3 Intelligent-Tiering will automatically move objects that haven't been accessed for 90 consecutive days to the Archive Access tier and then after 180 consecutive days of no access to the Deep Archive Access tier. If the objects are accessed later, S3 Intelligent-Tiering moves the objects back to the Frequent Access tier.

There are no retrieval fees when using the S3 Intelligent-Tiering storage class, and no additional tiering fees when objects are moved between access tiers within S3 Intelligent-Tiering. It is the ideal storage class for data sets with unknown storage access patterns, like new applications, or unpredictable access patterns, like data lakes.

Incorrect options:

Amazon S3 Standard (S3 Standard) - Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of

use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) - Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files.

Amazon S3 Random Access (S3 Random-Access) - This is a made-up option, given only as a distractor.

Reference:

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

✓ Which of the following statements is CORRECT regarding the scope of an Amazon Virtual Private Cloud (VPC)? *1/1

- ○ A VPC spans all AWS regions within an Availability Zone (AZ)
- ○ A VPC spans all Availability Zones (AZs) in all AWS regions
- ◉ A VPC spans all Availability Zones (AZs) within an AWS region ✓
- ○ Amazon VPC spans all subnets in all AWS regions

Feedback

Explanation
Correct option:

A VPC spans all Availability Zones (AZs) within an AWS region

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

An Amazon VPC spans all Availability Zones (AZs) within a region.

Incorrect options:

Amazon VPC spans all subnets in all AWS regions - A VPC is located within an AWS region.

A VPC spans all Availability Zones (AZs) in all AWS regions - A VPC is located within an AWS region.

A VPC spans all AWS regions within an Availability Zone (AZ) - AWS has the concept of a Region, which is a physical location around the world where AWS clusters data centers. Each AWS Region consists of multiple (two or more), isolated, and physically separate Availability Zone (AZs) within a geographic area. An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. Therefore, regions cannot be within an Availability Zone. Moreover, a VPC is located within a region.

AWS Regions and Availability Zones (AZs) Overview: via - https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Reference:

https://aws.amazon.com/vpc/

✓ A company has defined a baseline that mentions the number of AWS resources to be used for different stages of application testing. However, the company realized that employees are not adhering to the guidelines and provisioning additional resources via API calls, resulting in higher testing costs. *1/1

Which AWS service will help the company raise alarms whenever the baseline resource numbers are crossed?

- ○ AWS X-Ray
- ○ Amazon Detective
- ◉ AWS CloudTrail Insights ✓
- ○ AWS Config

Feedback

Explanation
Correct option:

AWS CloudTrail Insights

AWS CloudTrail Insights helps AWS users identify and respond to unusual activity associated with write API calls by continuously analyzing CloudTrail management events.

Insights events are logged when AWS CloudTrail detects unusual write management API activity in your account. If you have CloudTrail Insights enabled, and CloudTrail detects unusual activity, Insights events are delivered to the destination S3 bucket for your trail. You can also see the type of insight and the incident time period when you view Insights events on the CloudTrail console. Unlike other types of events captured in a CloudTrail trail, Insights events are logged only when CloudTrail detects changes in your account's API usage that differ significantly from the account's typical usage patterns.

AWS CloudTrail Insights can help you detect unusual API activity in your AWS account by raising Insights events. CloudTrail Insights measures your normal patterns of API call volume, also called the baseline, and generates Insights events when the volume is outside normal patterns.

AWS CloudTrail Insights continuously monitors CloudTrail write management events, and uses mathematical models to determine the normal levels of API and service event activity for an account. CloudTrail Insights identifies behavior that is outside normal patterns, generates Insights events, and delivers those events to a /CloudTrail-Insight folder in the chosen destination S3 bucket for your trail. You can also access and view Insights events in the AWS Management Console for CloudTrail.

Identify and Respond to Unusual API Activity using AWS CloudTrail Insights: via - https://aws.amazon.com/blogs/aws/announcing-cloudtrail-insights-identify-and-respond-to-unusual-api-activity/

Incorrect options:

AWS X-Ray - AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components. X-Ray is not for tracking user actions when interacting with the AWS systems.

Amazon Detective - Amazon Detective simplifies the process of investigating security findings and identifying the root cause. Amazon Detective analyzes trillions of events from multiple data sources such as VPC Flow Logs, AWS CloudTrail logs, and Amazon GuardDuty findings and automatically creates a graph model that provides you with a unified, interactive view of your resources, users, and the interactions between them over time.

AWS Config - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Reference:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-insights-events-with-cloudtrail.html

✓ An eCommerce company plans to use the AWS Cloud to quickly deliver new functionality in an iterative manner, minimizing the time to market. *1/1

Which feature of the AWS Cloud provides this functionality?

- (●) Agility ✓
- ( ) Cost effectiveness
- ( ) Fault tolerance
- ( ) Elasticity

Feedback

Explanation
In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes.

This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

CORRECT: "Agility" is the correct answer.

INCORRECT: "Elasticity" is incorrect. Elasticity enables infrastructure to scale based on demand and helps applications perform and be cost effective. It does not reduce time to market.

INCORRECT: "Fault tolerance" is incorrect as this is involved with ensuring applications stay available in the event of a fault.

INCORRECT: "Cost effectiveness" is incorrect. The AWS Cloud can be cost effective but this is not the benefit that allows faster time to market.

References:

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

✓ Which AWS tool/service will help you define your cloud infrastructure using popular programming languages such as Python and JavaScript? *1/1

- (●) AWS Cloud Development Kit (AWS CDK) ✓
- ( ) AWS Elastic Beanstalk
- ( ) AWS CloudFormation
- ( ) AWS CodeBuild

Feedback

Explanation
Correct option:

AWS Cloud Development Kit (AWS CDK)

The AWS Cloud Development Kit (AWS CDK) is an open-source software development framework to define your cloud application resources using familiar programming languages.

AWS Cloud Development Kit (AWS CDK) uses the familiarity and expressive power of programming languages for modeling your applications. It provides you with high-level components called constructs that preconfigure cloud resources with proven defaults, so you can build cloud applications without needing to be an expert. AWS CDK provisions your resources in a safe, repeatable manner through AWS CloudFormation. It also enables you to compose and share your own custom constructs that incorporate your organization's requirements, helping you start new projects faster.

In short, you use the AWS CDK framework to author AWS CDK projects which are executed to generate AWS CloudFormation templates.

How Cloud Development Kit (AWS CDK) works: via - https://aws.amazon.com/cdk/

Incorrect options:

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, etc. You can simply upload your code in a programming language of your choice and AWS Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, and auto scaling to application health monitoring.

AWS CloudFormation - AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS and third-party resources, and provision and manage them in an orderly and predictable fashion. AWS CloudFormation is designed to allow resource lifecycles to be managed repeatably, predictably, and safely while allowing for automatic rollbacks, automated state management, and management of resources across accounts and regions. AWS Cloud Development Kit (AWS CDK) helps code the same in higher-level languages and converts them into AWS CloudFormation templates.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that

compiles source code, runs tests, and produces software packages that are ready to deploy. With AWS CodeBuild, you don't need to provision, manage, and scale your own build servers. AWS CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue.

Reference:

https://aws.amazon.com/cdk/

✓ Which of the following points have to be considered when choosing an AWS Region for a service? (Select two) *1/1

- [x] Compliance and Data Residency guidelines of the AWS Region should match your business requirements ✓
- [ ] The AWS Region with high availability index should be considered for your business
- [x] AWS Region chosen should be geographically closer to the user base that utilizes the hosted AWS services ✓
- [ ] The AWS Region chosen should have all its Availability Zones (AZ) within 100 Kms radius, to keep latency low for hosted applications
- [ ] The AWS Region should have 5G networks, to seamlessly access the breadth of AWS services in the region

Feedback

Explanation
Correct options:

Compliance and Data Residency guidelines of the AWS Region should match your business requirements

If you have data residency requirements, you can choose the AWS Region that is in close proximity to your desired location. You retain complete control and ownership over the region in which your data is physically located, making it easy to meet regional compliance and data residency requirements.

AWS Region chosen should be geographically closer to the user base that utilizes the hosted AWS services

When deploying your applications and workloads to the cloud, you have the flexibility in selecting a technology infrastructure and AWS Region that is closest to your primary target of users.

Incorrect options:

The AWS Region with high availability index should be considered for your business - AWS delivers the highest network availability of any cloud provider. Each region is fully isolated and comprised of multiple Availability Zone (AZs), which are fully isolated partitions of our infrastructure. All AWS Regions are designed to be highly available.

The AWS Region should have 5G networks, to seamlessly access the breadth of AWS services in the region - AWS Local Zones and AWS Wavelength, with telco providers, provide performance for applications that require single-digit millisecond latencies by delivering AWS infrastructure and services closer to end-users and 5G connected devices. But, having a 5G network is not a factor for a customer to decide on an AWS Region.

The AWS Region chosen should have all its Availability Zones (AZ) within 100 Kms radius, to keep latency low for hosted applications - An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. AZ's are physically separated by a meaningful distance, many kilometers, from any

other Availability Zone (AZ), although all are within 100 km (60 miles) of each other. This applies to all Availability Zones (AZ) and hence is not a criterion for choosing an AWS Region.

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

✓ Which security control tool can be used to deny traffic from a specific IP address? *1/1

- (●) Network Access Control List (network ACL) ✓
- ( ) Security Group
- ( ) Amazon GuardDuty
- ( ) VPC Flow Logs

Feedback

Explanation
Correct option:

Network Access Control List (network ACL)

A Network Access Control List (network ACL) is an optional layer of security for your virtual private cloud (VPC) that acts as a firewall for controlling traffic in and out of one or more subnets (i.e. it works at the subnet level). A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.

Network Access Control List (network ACL) Overview: via -
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Incorrect options:

Security Group - A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. Security groups act at the instance level, not at the subnet level. You can specify allow rules, but not deny rules. You can specify separate rules for inbound and outbound traffic.

Amazon GuardDuty - Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. Amazon GuardDuty also detects potentially compromised instances or reconnaissance by attackers. It cannot deny traffic from a specific IP address.

VPC Flow Logs - VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon Simple Storage Service (Amazon S3). After you've created a flow log, you can retrieve and view its data in the chosen destination. However, it cannot deny traffic from a specific IP address.

Reference:

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

✓ Which of the following statements are correct regarding the health monitoring and reporting capabilities supported by AWS Elastic Beanstalk? (Select two) *1/1

- [x] With basic health reporting, the AWS Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch ✓
- [x] The AWS Elastic Beanstalk health monitoring can determine that the environment's Auto Scaling group is available and has a minimum of at least one instance ✓
- [ ] The basic health reporting system that provides information about the health of instances in an AWS Elastic Beanstalk environment does not use health checks performed by Elastic Load Balancing (ELB)
- [ ] AWS Elastic Beanstalk provides only basic health reporting system; Combined with Elastic Load Balancing (ELB), they provide advanced health check features
- [ ] In a single instance environment, AWS Elastic Beanstalk determines the instance's health by monitoring the Elastic Load Balancing (ELB) health settings

Feedback

Explanation
Correct options:

The AWS Elastic Beanstalk health monitoring can determine that the environment's Auto Scaling group is available and has a minimum of at least one instance

In addition to Elastic Load Balancing health checks, AWS Elastic Beanstalk monitors resources in your environment and changes health status to red if they fail to deploy, are not configured correctly, or become unavailable. These checks confirm that: 1. The environment's Auto Scaling group is available and has a minimum of at least one instance. 2. The environment's security group is available and is configured to allow incoming traffic on port 80. 3. The environment CNAME exists and is pointing to the right load balancer. 4. In a worker environment, the Amazon Simple Queue Service (Amazon SQS) queue is being polled at least once every three minutes.

With basic health reporting, the AWS Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch

With basic health reporting, the AWS Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch. The CloudWatch metrics used to produce graphs on the Monitoring page of the environment console are published by the resources in your environment.

Incorrect options:

AWS Elastic Beanstalk provides only basic health reporting system; Combined with Elastic Load Balancing (ELB), they provide advanced health check features - This option has been added as a distractor.

In a single instance environment, AWS Elastic Beanstalk determines the instance's health

by monitoring the Elastic Load Balancing (ELB) health settings - In a single instance or worker tier environment, AWS Elastic Beanstalk determines the instance's health by monitoring its Amazon EC2 instance status. Elastic Load Balancing health settings, including HTTP health check URLs cannot be used in these environment types.

The basic health reporting system that provides information about the health of instances in an AWS Elastic Beanstalk environment does not use health checks performed by Elastic Load Balancing (ELB) - The basic health reporting system provides information about the health of instances in an AWS Elastic Beanstalk environment based on health checks performed by Elastic Load Balancing for load-balanced environments, or Amazon Elastic Compute Cloud (Amazon EC2) for single-instance environments.

Reference:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.healthstatus.html#monitoring-basic-additionalchecks

✓ Which of the following AWS services are offered free of cost? (Select two) *1/1

- [x] AWS Elastic Beanstalk ✓
- [ ] Amazon CloudWatch facilitated detailed monitoring of EC2 instances
- [x] AWS Auto Scaling ✓
- [ ] Amazon EC2 Spot Instances
- [ ] An Elastic IP address, which is chargeable as long as it is associated with an EC2 instance

Feedback

Explanation
Correct options:

AWS Elastic Beanstalk

There is no additional charge for AWS Elastic Beanstalk. You pay for AWS resources (e.g. EC2 instances or S3 buckets) you create to store and run your application. You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

AWS Auto Scaling

There is no additional charge for AWS Auto Scaling. You pay only for the AWS resources needed to run your applications and Amazon CloudWatch monitoring fees.

Incorrect options:

Amazon EC2 Spot Instances - Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices. Spot Instances are, however, not free.

Amazon CloudWatch facilitated detailed monitoring of EC2 instances - If you enable detailed monitoring, you are charged per metric that is sent to CloudWatch. You are not charged for data storage. Data is available in 1-minute periods, as opposed to 5-minute periods at no charge, for basic monitoring.

An Elastic IP address, which is chargeable as long as it is associated with an EC2 instance - An Elastic IP address doesn't incur charges as long as all the following conditions are true: The Elastic IP address is associated with an EC2 instance, The instance associated with the Elastic IP address is running, The instance has only one Elastic IP address attached to it and the Elastic IP address is associated with an attached network interface, such as a Network Load Balancer or NAT gateway.

References:

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

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-new.html

https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/

✓ Which AWS service allows you to quickly and easily add user sign-up, sign-in, and access control to web and mobile applications? *1/1

- ○ AWS Organizations
- ○ AWS IAM Identity Center
- ◉ Amazon Cognito ✓
- ○ AWS Identity and Access Management (AWS IAM)

Feedback

Explanation
Correct option:

Amazon Cognito

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. With Amazon Cognito, you also have the option to authenticate users through social identity providers such as Facebook, Twitter, or Amazon, with SAML identity solutions, or by using your own identity system.

Incorrect options:

AWS Identity and Access Management (AWS IAM) - AWS Identity and Access Management (AWS IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. It does not provide user sign-up, sign-in, and access control to web and mobile applications.

AWS IAM Identity Center - AWS IAM Identity Center is the successor to AWS Single Sign-On. It is built on top of AWS Identity and Access Management (IAM) to simplify access management to multiple AWS accounts, AWS applications, and other SAML-enabled cloud applications. In IAM Identity Center, you create, or connect, your workforce users for use across AWS. You can choose to manage access just to your AWS accounts, just to your cloud applications, or to both.

AWS Organizations - AWS Organizations offers policy-based management for multiple AWS accounts. With AWS Organizations, you can create groups of accounts, automate account creation, and apply and manage policies for those groups. Organizations enable you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes. It does not provide user sign-up, sign-in, and access control to web and mobile applications.

Reference:

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

✓ Historically, IT departments had to over-provision for peak demand. IT professionals may bring this legacy mindset to the table when they build their cloud infrastructure leading to over-provisioned resources and unnecessary costs. Right-sizing of resources is necessary to reduce infrastructure costs while still using cloud functionality optimally. *1/1

Which feature of the AWS Cloud refers to right-sizing the resources?

- ○ Resiliency
- ◉ Elasticity ✓
- ○ Horizontal scaling
- ○ Reliability

Feedback

Explanation
Correct option:

Elasticity

Most people, when thinking of cloud computing, think of the ease with which they can procure resources when needed. This is only one aspect of elasticity. The other aspect is to contract when they no longer need resources. Scale-out and scale in. Scale up and scale down.

The ability to acquire resources as you need them and release resources when you no longer need them. In the cloud, you want to do this automatically.

Some AWS services do this as part of their service: Amazon Simple Storage Service (Amazon S3), Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS), Amazon Simple Email Service (Amazon SES), Amazon Aurora, etc. Some require vertical scaling, like Amazon Relational Database Service (Amazon RDS). Others integrate with AWS Auto Scaling, like Amazon EC2, Amazon ECS, AWS Fargate, Amazon EKS, and Amazon DynamoDB. Amazon Aurora Serverless and Amazon Athena also qualify as elastic.

Incorrect options:

Reliability - The ability of a workload to perform its intended function correctly and consistently when it's expected to. This includes the ability to operate and test the workload through its total lifecycle.

Resiliency - The ability of a workload to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions, such as misconfigurations or transient network issues.

Horizontal scaling - A "horizontally scalable" system can increase capacity by adding more computers to the system. This is in contrast to a "vertically scalable" system, which is constrained to running its processes on only one computer; in such systems, the only way

to increase performance is to add more resources into one computer in the form of faster (or more) CPUs, memory or storage.

References:

https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html

https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concepts.wa-concepts.en.html

✗ AWS Support offers five support plans for its customers. Which of the following features are covered as part of the AWS Basic Support Plan? (Select two) *0/1

- [ ] One-on-one responses to account and billing questions
- [ ] infrastructure event management
- [x] Use-case guidance – What AWS products, features, and services to use for best supporting your specific needs ✗
- [ ] Client-side diagnostic tools
- [x] Service health checks ✓

Correct answer

- [x] One-on-one responses to account and billing questions
- [x] Service health checks

Feedback

Explanation
Correct options:

One-on-one responses to account and billing questions

Service health checks

AWS Support offers five support plans: Basic support plan, AWS Developer support plan, AWS Business support plan, AWS Enterprise-On-Ramp support plan, and AWS Enterprise Support plan.

The Basic plan offers support for account and billing questions and service quota increases. The other plans offer a number of technical support cases with pay-by-the-month pricing and no long-term contracts. All AWS customers automatically have 24/7 access to these features of the Basic support plan: 1. One-on-one responses to account and billing questions 2. Support forums 3. Service health checks 4. Documentation, technical papers, and best practice guides

via - https://docs.aws.amazon.com/awssupport/latest/user/aws-support-plans.html

Incorrect options:

Client-side diagnostic tools - Customers with any of the Developer, Business, Enterprise-On-Ramp, Enterprise support plans have access to client-side diagnostic tools.

Use-case guidance – What AWS products, features, and services to use for best supporting your specific needs - Customers with any of the Business, Enterprise-On-Ramp, Enterprise support plans have access to use-case guidance.

Infrastructure event management - Customers with AWS Enterprise-On-Ramp or Enterprise

support plan have access to infrastructure event management which is a short-term engagement with AWS Support to get a deep understanding of customer use-cases. After analysis, AWS provides architectural and scaling guidance for an event.

References:

https://docs.aws.amazon.com/awssupport/latest/user/aws-support-plans.html

https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html

✓ A company provides you with a completed product that is run and managed by the company itself. As a customer, you only use the product without worrying about maintaining or managing the product. *1/1

Which cloud computing model does this kind of product belong to?

- ○ Infrastructure as a Service (IaaS)
- ◉ Software as a Service (SaaS) ✓
- ○ Platform as a Service (PaaS)
- ○ Product as a Service (Paas)

Feedback

Explanation
Correct option:

Software as a Service (SaaS)

Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering, you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece of software.

A common example of a SaaS application is the web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

Incorrect options:

Infrastructure as a Service (IaaS) - Infrastructure as a service (IaaS), sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.

Platform as a Service (PaaS) - Platform as a Service (PaaS) as a service removes the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

Product as a Service (Paas) - This is a made-up option, given only as a distractor.

Reference:

https://aws.amazon.com/types-of-cloud-computing/

✓ A company would like to define a set of rules to manage objects cost-effectively between Amazon Simple Storage Service (Amazon S3) storage classes. As a Cloud Practitioner, which Amazon S3 feature would you use? *1/1

- (●) Amazon Simple Storage Service (Amazon S3) Lifecycle configuration ✓
- ( ) Amazon S3 Transfer Acceleration (Amazon S3TA)
- ( ) S3 Cross-Region Replication (S3 CRR)
- ( ) Amazon Simple Storage Service (Amazon S3) Bucket policies

Feedback

Explanation
Correct option:

Amazon Simple Storage Service (Amazon S3) Lifecycle configuration

To manage your objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions: Transition actions (define when objects transition to another storage class) and expiration actions (define when objects expire. Amazon S3 deletes expired objects on your behalf).

In this particular use case, you would use a transition action.

Incorrect options:

Amazon S3 Transfer Acceleration (Amazon S3TA) - Amazon S3 Transfer Acceleration (Amazon S3TA) enables fast, easy, and secure transfers of files over long distances between your client and an Amazon S3 bucket. It is not used to move objects between storage classes.

Amazon Simple Storage Service (Amazon S3) Bucket policies - An S3 bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates. It is not used to move objects between storage classes.

S3 Cross-Region Replication (S3 CRR) - S3 Cross-Region Replication (S3 CRR) enables automatic, asynchronous copying of objects across Amazon S3 buckets. Cross-Region replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions. It is not used to move objects between storage classes.

References:

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

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

✓ A Security Group has been changed in an AWS account and the manager of the account has asked you to find out the details of the user who changed it. As a Cloud Practitioner, which AWS service will you use to fetch the necessary information? *1/1

- ○ Amazon Inspector
- ○ AWS Trusted Advisor
- ◉ AWS CloudTrail ✓
- ○ AWS X-Ray

Feedback

Explanation
Correct option:

AWS CloudTrail

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

AWS CloudTrail provides visibility into user activity by recording actions taken on your account. CloudTrail records important information about each action, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. This information helps you to track changes made to your AWS resources and to troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.

How AWS CloudTrail Works: via - https://aws.amazon.com/cloudtrail/

Incorrect options:

AWS X-Ray - AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components. X-Ray is not for tracking user actions when interacting with the AWS systems.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make

security testing a more regular occurrence as part of the development and IT operations.

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

Reference:

https://aws.amazon.com/cloudtrail/

✓ A company needs to use third-party software for its workload on AWS. *1/1

Is there a feature or service of AWS that the company can use to purchase the software?

- AWS Resource Access Manager
- AWS Managed Services
- AWS Marketplace ✓
- AWS License Manager

Feedback

Explanation
AWS Marketplace is a curated digital catalog that makes it easy for organizations to discover, procure, entitle, provision, and govern third-party software. You can find thousands of software listings from popular categories like security, business applications, and data & analytics, and across specific industries, such as healthcare, financial services, and public sector.

CORRECT: "AWS Marketplace" is the correct answer (as explained above.)

INCORRECT: "AWS Managed Service" is incorrect as this describes services in which AWS customers don't have to provision their own infrastructure.

INCORRECT: "AWS License Manager" is incorrect as it is a service that makes it easier for you to manage Software Licenses.

INCORRECT: "AWS Resource Access Manager" is incorrect as it is a service that helps you to securely share your resources across AWS accounts, within your organization or organizational units (OUs) within AWS and has nothing to do with third party services.

References:

https://aws.amazon.com/mp/marketplace-service/overview/

✗ Which of the following statements are correct regarding the AWS Support Plans? (Select two) *0/1

- [x] AWS Concierge service is available for the AWS Business Support and AWS Enterprise Support plans ✗
- [ ] Contextual guidance based on customer use-case, is available only for the AWS Enterprise support plan
- [ ] Infrastructure Event Management is included for free for AWS Business Support and AWS Enterprise Support plans and can be extended to AWS Developer Support plan for an additional fee
- [x] A designated Technical Account Manager is available only for AWS Enterprise Support plan ✓
- [ ] Both Basic and AWS Developer Support plans have access to the core Trusted Advisor checks only

Correct answer

- [x] A designated Technical Account Manager is available only for AWS Enterprise Support plan
- [x] Both Basic and AWS Developer Support plans have access to the core Trusted Advisor checks only

Feedback

Explanation
Correct options:

A designated Technical Account Manager is available only for AWS Enterprise Support plan

A designated Technical Account Manager (TAM) is the primary point of contact who provides guidance, architectural review, and ongoing communication to keep the customer informed and well prepared as they plan, deploy, and proactively optimize their AWS solutions. As the cornerstone of the Enterprise Support plan, your TAM serves as your guide and advocate, focused on delivering the right resources to support the success and ongoing operational health of your AWS infrastructure.

Both Basic and AWS Developer Support plans have access to the core Trusted Advisor checks only

AWS Trusted Advisor draws upon best practices learned from the aggregated operational history of serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and alerts you to opportunities to save money, improve system availability and performance, or help close security gaps. Access to the core Trusted Advisor checks, and guidance to provision your resources following best practices to increase performance and improve security are only part of the Basic and Developer support plans.

Incorrect options:

AWS Concierge service is available for the AWS Business Support and AWS Enterprise Support plans - AWS Concierge is a senior customer service agent who is assigned to your account when you subscribe to an Enterprise or qualified Reseller Support plan. This Concierge agent is your primary point of contact for billing or account inquiries; when you don't know whom to call, they will find the right people to help. In most cases, the AWS Concierge is available during regular business hours in your headquarters' geography.

Contextual guidance based on customer use-case, is available only for the AWS Enterprise support plan - Contextual guidance on how services fit together to meet your specific use-case, workload, or application is part of the Business support plan.

Infrastructure Event Management is included for free for AWS Business Support and AWS Enterprise Support plans and can be extended to AWS Developer Support plan for an additional fee - AWS Infrastructure Event Management is a short-term engagement with AWS Support, available as part of the Enterprise-level Support product offering (also available to the AWS Enterprise On-Ramp Support plan subject to a cap of one per year), and available for additional purchase for AWS Business Support plan users. AWS Infrastructure Event Management partners with your technical and project resources to gain a deep understanding of your use case and provide architectural and scaling guidance for an event. Common use-case examples for AWS Event Management include advertising launches, new product launches, and infrastructure migrations to AWS. Infrastructure Event Management cannot be extended to a AWS Developer Support plan for an additional fee.

Reference:

https://aws.amazon.com/premiumsupport/plans/

✓ Which Amazon EC2 pricing model should be used to comply with per-core software license requirements? *1/1

- ( ) Reserved Instances
- (•) Dedicated Hosts ✓
- ( ) Spot Instances
- ( ) On-Demand Instances

Feedback

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

CORRECT: "Dedicated Hosts" is the correct answer.

INCORRECT: "On-Demand Instances" is incorrect. This is a standard pricing model and does not offer the advantages requested.

INCORRECT: "Spot Instances" is incorrect. This is used to obtain discounted pricing for short-term requirements that can be interrupted.

INCORRECT: "Reserved Instances" is incorrect. This is used to lower cost by reserving usage of an instance for a term of 1 or 3 years.

References:

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

✓ A company wants to utilize a pay as you go cloud model for all of their applications without CAPEX costs and which is highly elastic. Which cloud delivery model will suit them best? *1/1

- ○ On-premise
- ○ Private
- ○ Hybrid
- ◉ Public ✓

Feedback

Explanation
The public cloud is offered under a purely pay as you go model (unless you choose to reserve), and allows companies to completely avoid CAPEX costs. The public cloud is also highly elastic so companies can grow and shrink the applications as demand changes.

Private and on-premise clouds are essentially the same, though both could be managed by a third party and even could be delivered under an OPEX model by some vendors. However, they are typically more CAPEX heavy and the elasticity is limited.

A hybrid model combines public and private and this company wants to go all in on a single model.

CORRECT: "Public" is the correct answer.

INCORRECT: "Private" is incorrect as explained above.

INCORRECT: "Hybrid" is incorrect as explained above.

INCORRECT: "On-premise" is incorrect as explained above.

References:

https://aws.amazon.com/types-of-cloud-computing/

✓ Which service can be used to assign a policy to a group? * 1/1

- (●) AWS IAM ✓
- ( ) AWSn STS
- ( ) AWS Shield
- ( ) Amazon Cognito

Feedback

Explanation
IAM is used to securely control individual and group access to AWS resources. Groups are collections of users and have policies attached to them. You can use IAM to attach a policy to a group

CORRECT: "AWS IAM" is the correct answer.

INCORRECT: "Amazon Cognito" is incorrect. Amazon Cognito is used for authentication using mobile apps

INCORRECT: "AWS STS" is incorrect. The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users)

INCORRECT: "AWS Shield" is incorrect. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

References:

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

✓ Which of the following AWS services can be used to generate, use, and manage encryption keys on the AWS Cloud? *1/1

- ○ Amazon Inspector
- ○ AWS Secrets Manager
- ◉ AWS CloudHSM ✓
- ○ AWS GuardDuty

Feedback

Explanation
Correct option:

AWS CloudHSM

The AWS CloudHSM service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud.

AWS CloudHSM allows you to securely generate, store, and manage cryptographic keys used for data encryption in a way that keys are accessible only to you.

How AWS CloudHSM works: via - https://aws.amazon.com/cloudhsm/

Incorrect options:

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. It cannot be used to generate, use, and manage encryption keys.

AWS GuardDuty - Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It cannot be used to generate, use, and manage encryption keys.

AWS Secrets Manager - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. It is integrated with AWS CloudHSM to generate, use, and manage encryption keys.

Reference:

https://aws.amazon.com/cloudhsm/

✓ Which of the following AWS services can be used to continuously monitor both malicious activities as well as unauthorized behavior to protect your AWS accounts and workloads? *1/1

- ○ AWS Security Hub
- ○ Amazon Inspector
- ◉ Amazon GuardDuty ✓
- ○ Amazon Detective

Feedback

Explanation
Correct option:

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon Simple Storage Service (Amazon S3). With the cloud, the collection and aggregation of account and network activities are simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. With Amazon GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS.

The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain.

Amazon GuardDuty makes it easy for you to enable continuous monitoring of your AWS accounts, workloads, and data stored in Amazon S3. It operates completely independently from your resources so there is no risk of performance or availability impacts to your workloads. It's fully managed with integrated threat intelligence, anomaly detection, and machine learning. Amazon GuardDuty delivers detailed and actionable alerts that are easy to integrate with existing event management and workflow systems. There are no upfront costs and you pay only for the events analyzed, with no additional software to deploy or subscriptions to threat intelligence feeds required.

How Amazon GuardDuty Works: via - https://aws.amazon.com/guardduty/

Incorrect options:

AWS Security Hub - AWS Security Hub gives you a comprehensive view of your security alerts and security posture across your AWS accounts. There is a range of powerful security tools at your disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. With Security Hub, you have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions.

Amazon Detective - Amazon Detective simplifies the process of investigating security findings and identifying the root cause. Amazon Detective analyzes trillions of events from multiple data sources such as VPC Flow Logs, AWS CloudTrail logs, and Amazon GuardDuty findings and automatically creates a graph model that provides you with a unified, interactive view of your resources, users, and the interactions between them over time.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of the development and IT operations.

References:

https://aws.amazon.com/guardduty/

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

✓ Which of the following should be used to improve the security of access to the AWS Management Console? (Select TWO.) *1/1

- [x] AWS Multi-Factor Authentication (AWS MFA) ✓
- [ ] AWS Certificate Manager
- [x] Strong password policies ✓
- [ ] AWS Secrets Manager
- [ ] Security group rules

Feedback

Explanation
For extra security, AWS recommends that you require multi-factor authentication (MFA) for all users in your account. With MFA, users have a device that generates a response to an authentication challenge.

Both the user's credentials (something you know) and the device-generated response (something you have) are required to complete the sign-in process. If a user's password or access keys are compromised, your account resources are still secure because of the additional authentication requirement.

Additionally, strong password policies should be used to enforce measures including minimum password length, complexity, and password reuse restrictions.

CORRECT: "AWS Multi-Factor Authentication (AWS MFA)" is a correct answer.

CORRECT: "Strong password policies" is also a correct answer.

INCORRECT: "AWS Secrets Manager" is incorrect. This service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

INCORRECT: "AWS Certificate Manager" is incorrect. This service is used for creating SSL/TLS certificates for use with HTTPS connections.

INCORRECT: "Security group rules" is incorrect as these are used to restrict traffic to/from your EC2 instances.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

✓ A company based in Sydney hosts its application on an Amazon Elastic Compute Cloud (Amazon EC2) instance in ap-southeast-2. They would like to deploy the same Amazon EC2 instances in eu-south-1. Which of the following AWS entities can address this use case? *1/1

- ○ Elastic Load Balancing (ELB)
- ○ AWS Lambda
- ○ Amazon EBS Elastic Volume snapshots
- ◉ Amazon Machine Image (AMI) ✓

Feedback

Explanation
Correct option:

Amazon Machine Image (AMI)

An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an Amazon Machine Image (AMI) when you launch an instance. You can launch multiple instances from a single Amazon Machine Image (AMI) when you need multiple instances with the same configuration.

How to use an Amazon Machine Image (AMI): via -
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Incorrect options:

Elastic Load Balancing (ELB) - Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone (AZ) or across multiple Availability Zones (AZs). It cannot be used to deploy the same EC2 instances across different Availability Zones (AZs).

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. It cannot be used to deploy the same EC2 instances across different Availability Zones (AZs).

Amazon EBS Elastic Volume snapshots - An Amazon EBS snapshot is a point-in-time copy of your Amazon EBS volume. EBS snapshots are one of the components of an AMI, but EBS snapshots alone cannot be used to deploy the same EC2 instances across different Availability Zones (AZs).

Reference:

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

✓ Who is accountable for security and compliance under the AWS shared responsibility model? *1/1

- ○ The customer is responsible.
- ○ AWS is responsible.
- ◉ AWS and the customer share responsibility. ✓
- ○ AWS shares responsibility with the relevant governing body.

Feedback

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help
relieve the customer's operational burden as
AWS operates, manages and controls the components from the host operating system and virtualization layer
down to the physical security of the facilities in which the service operates.

✓ A blogging company is looking at an easy to use solution to host WordPress blogs. The company needs a cost-effective, readily available solution without the need to manage the configurations for servers or the databases. *1/1

Which AWS service will help you achieve this functionality?

- ○ Host the application directly on Amazon S3
- ◉ Amazon Lightsail ✓
- ○ AWS Fargate
- ○ Amazon Elastic Compute Cloud (EC2) with Amazon S3 for storage

Feedback

Explanation
Correct option:

Amazon Lightsail

Amazon Lightsail is the easiest way to get started with AWS for developers, small businesses, students, and other users who need a solution to build and host their applications on the cloud. Lightsail provides developers with compute, storage, and networking capacity and capabilities to deploy and manage websites and web applications in the cloud. Lightsail includes everything you need to launch your project quickly – virtual machines, containers, databases, CDN, load balancers, DNS management, etc. – for a low, predictable monthly price.

You can get preconfigured virtual private server (VPS) plans that include everything to easily deploy and manage your application. Amazon Lightsail is best suited to projects that require a few virtual private servers and users who prefer a simple management interface. Common use cases for Lightsail include running websites, web applications, blogs, e-commerce sites, simple software, and more.

Also referred to as a bundle, a Lightsail plan includes a virtual server with a fixed amount of memory (RAM) and compute (vCPUs), SSD-based storage (disks), and a free data transfer allowance. Amazon Lightsail plans also offer static IP addresses (5 per account) and DNS management (3 domain zones per account). Lightsail plans are charged on an hourly, on-demand basis, so you only pay for a plan when you're using it.

Amazon Lightsail offers a number of preconfigured, one-click-to-launch operating systems, development stacks, and web applications, including Linux and Windows OS, WordPress, LAMP, CentOS, and more.

Incorrect options:

AWS Fargate - AWS Fargate is a serverless compute engine for containers that work with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources

per application, and improves security through application isolation by design. Fargate is meant for container applications that you wish to host without having to manage the servers such as EC2 instances.

Amazon Elastic Compute Cloud (EC2) with Amazon S3 for storage - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

Amazon EC2 instances need to be managed by the customers and hence is the wrong choice for the given scenario.

Host the application directly on Amazon S3 - Amazon S3 does not support compute capacity to generate dynamic content. Only static web applications can be hosted on Amazon S3.

References:

https://aws.amazon.com/lightsail/

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

✓ Which of the following are architectural best practices for the AWS Cloud? (Select TWO.) *1/1

- [ ] Close coupling
- [x] Deploy into multiple Availability Zones ✓
- [ ] Deploy into a single availability zone
- [ ] Create monolithic architectures
- [x] Design for fault tolerance ✓

Feedback

Explanation
It is an architectural best practice to deploy your resources into multiple availability zones and design for fault tolerance. These both ensure that if resources or infrastructure fails, your application continues to run.

CORRECT: "Deploy into multiple Availability Zones" is a correct answer.

CORRECT: "Design for fault tolerance" is also a correct answer.

INCORRECT: "Deploy into a single availability zone" is incorrect. You should not deploy all of your resources into a single availability zone as any infrastructure failure will take down access to your resources.

INCORRECT: "Close coupling" is incorrect. Close coupling is not an architectural best practice – loose coupling is. With loose coupling you reduce interdependencies between components of an application and often put a middle layer such as a message bus between components.

INCORRECT: "Create monolithic architectures" is incorrect. You should not create monolithic architectures. With monolithic architectures you have a single instance running multiple components of the application, if any of these components fails, your application fails. It is better to design microservices architectures where components are spread across more instances.

References:

https://aws.amazon.com/architecture/well-architected/

✓ Which benefit of AWS enables companies to replace upfront fixed expenses with variable expenses when using on-demand technology services? *1/1

- ○ Economies of scale
- ○ High availability
- ◉ Pay-as-you-go pricing ✓
- ○ Global reach

Feedback

Explanation
Pay-as-you-go-pricing is an example of the AWS advantage "Trade capital expense for variable expense". This is documented in the Six Advantages of Cloud Computing.

Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can pay only when you consume computing resources, and pay only for how much you consume.

CORRECT: "Pay-as-you-go pricing" is the correct answer.

INCORRECT: "Economies of scale" is incorrect. This is not an example of replacing fixed expenses with variable expenses. The benefit of economies of scale relates to achieving a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay as-you-go prices.

INCORRECT: "Global reach" is incorrect. This is most closely associated with the advantage "Go global in minutes". With AWS you can easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide lower latency and a better experience for your customers at minimal cost.

INCORRECT: "High availability" is incorrect. High availability is not related to pricing. Instead, it means you can design your applications to be available with minimum downtime even when disruptions occur.

References:

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

✓ Which of the following are the security best practices suggested by AWS for Identity and Access Management (IAM)? (Select two) *1/1

- [x] Do not share security credentials between accounts, use IAM roles instead ✓
- [ ] Enable AWS Multi-Factor Authentication (AWS MFA) on your AWS root user account. MFA helps give root access to multiple users without actually sharing the root user login credentials
- [ ] Share your AWS account root user credentials only if absolutely necessary for performing an important billing operation
- [ ] Do not change passwords and access keys once created. This results in failure of connectivity in the application logic
- [x] When you create IAM policies, grant the least privileges required to perform a task ✓

Feedback

Explanation
Correct options:

When you create IAM policies, grant the least privileges required to perform a task

When you create IAM policies, follow the standard security advice of granting the least privileges, or granting only the permissions required to perform a task. Determine what users (and roles) need to do and then craft policies that allow them to perform only those tasks.

Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later.

Do not share security credentials between accounts, use IAM roles instead

Don't share security credentials between accounts to allow users from another AWS account to access resources in your AWS account. Instead, use IAM roles. You can define a role that specifies what permissions the IAM users in the other account are allowed. You can also designate which AWS accounts have the IAM users that are allowed to assume the role.

Incorrect options:

Share your AWS account root user credentials only if absolutely necessary for performing an important billing operation - Never share your AWS account root user password or access keys with anyone. Don't use your AWS account root user credentials to access AWS, and don't give your credentials to anyone else. Instead, create individual users for anyone who needs access to your AWS account. Create an IAM user for yourself as well, give that user administrative permissions, and use that IAM user for all your work.

Enable AWS multi-factor authentication (MFA) on your AWS root user account. MFA helps give root access to multiple users without actually sharing the root user login credentials - The given option just acts as a distractor. For extra security, AWS recommends that you

use multi-factor authentication (MFA) for the root user in your account. With MFA, users have a device that generates a response to an authentication challenge. Both the user's credentials and the device-generated response are required to complete the sign-in process. If a user's password or access keys are compromised, your account resources are still secure because of the additional authentication requirement.

Do not change passwords and access keys once created. This results in failure of connectivity in the application logic - The given option just acts as a distractor. You should change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a custom password policy to your account to require all your IAM users to rotate their AWS Management Console passwords. You can also choose how often they must do so.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

✓ Which of the following is the least effort way to encrypt data for AWS services only in your AWS account using AWS Key Management Service (KMS)? *1/1

- ○ Create your own customer managed keys (CMKs) in AWS KMS
- ○ Use AWS owned CMK in the service you wish to use encryption
- ◉ Use AWS managed master keys that are automatically created in your account for each service ✓
- ○ Use AWS KMS APIs to encrypt data within your own application by using the AWS Encryption SDK

Feedback

Explanation
Correct option:

Use AWS managed master keys that are automatically created in your account for each service

AWS KMS keys (KMS keys) are the primary resource in AWS KMS. You can use a KMS key to encrypt, decrypt, and re-encrypt data. It can also generate data keys that you can use outside of AWS KMS. AWS KMS is replacing the term customer master key (CMK) with AWS KMS key and KMS key.

AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. Some AWS services support only an AWS managed CMK. Others use an AWS owned CMK or offer you a choice of CMKs. AWS managed CMK can be used only for your AWS account.

You can view the AWS managed CMKs in your account, view their key policies, and audit their use in AWS CloudTrail logs. However, you cannot manage these CMKs, rotate them, or change their key policies. And, you cannot use AWS managed CMKs in cryptographic operations directly; the service that creates them uses them on your behalf.

AWS managed CMKs appear on the AWS managed keys page of the AWS Management Console for AWS KMS. You can also identify most AWS managed CMKs by their aliases, which have the format aws/service-name, such as aws/redshift.

You do not pay a monthly fee for AWS managed CMKs. They can be subject to fees for use in excess of the free tier, but some AWS services cover these costs for you.

Incorrect options:

Create your own customer managed keys (CMKs) in AWS KMS - The AWS KMS keys that you create are customer managed keys. Customer managed keys are KMS keys in your AWS account that you create, own, and manage. You have full control over these KMS keys, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the KMS keys, and scheduling the KMS keys for deletion.

customer managed key (CMK) incur a monthly fee and a fee for use in excess of the free tier. They are counted against the AWS KMS quotas for your account.

Use AWS KMS APIs to encrypt data within your own application by using the AWS Encryption SDK - AWS KMS APIs can also be accessed directly through the AWS KMS Command Line Interface or AWS SDK for programmatic access. AWS KMS APIs can also be used indirectly to encrypt data within your own applications by using the AWS Encryption SDK. This requires code changes and is not the easiest way to achieve encryption.

Use AWS owned CMK in the service you wish to use encryption - AWS owned CMKs are a collection of CMKs that an AWS service owns and manages for use in multiple AWS accounts. Although AWS owned CMKs are not in your AWS account, an AWS service can use its AWS owned CMKs to protect the resources in your account. AWS owned CMK can be used for multiple AWS accounts.

You do not need to create or manage the AWS owned CMKs. However, you cannot view, use, track, or audit them. You are not charged a monthly fee or usage fee for AWS owned CMKs and they do not count against the AWS KMS quotas for your account.

Reference:

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

✓ Which statement is true in relation to data stored within an AWS Region? * 1/1

- ○ Data is always automatically replicated to at least one other availability zone
- ○ Data is automatically archived after 90 days
- ◉ Data is not replicated outside of a region unless you configure it ✓
- ○ Data is always replicated to another region

Feedback

Explanation
Data stored within an AWS region is not replicated outside of that region automatically. It is up to customers of AWS to determine whether they want to replicate their data to other regions. You must always consider compliance and network latency when making this decision.

CORRECT: "Data is not replicated outside of a region unless you configure it" is the correct answer.

INCORRECT: "Data is always replicated to another region" is incorrect. Data is never replicated outside of a region unless you configure it.

INCORRECT: "Data is automatically archived after 90 days" is incorrect. Data is never automatically archived. You must configure data to be archived.

INCORRECT: "Data is always automatically replicated to at least one other availability zone" is incorrect. Data is not automatically replicated to at least one availability zone – this is specific to each service and you must check how your data is stored and whether the availability and durability is acceptable.

References:

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

✓ Which Amazon EC2 tool acts as a virtual firewall to control inbound and outbound traffic to an EC2 instance? *1/1

- ○ Network access control list (ACL)
- ◉ Security group ✓
- ○ AWS WAF
- ○ AWS Shield

Feedback

Explanation
A security group acts as a virtual firewall, controlling the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

CORRECT: "Security Group" is the correct answer (as explained above.)

INCORRECT: "AWS Shield" is incorrect. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service and does not control traffic.

INCORRECT: "AWS WAF" is incorrect, as the WAF is a Web Application Firewall - something that is placed in front of your web applications outside of your VPC - whereas security groups live within your VPC, controlled instance specific inbound and outbound traffic.

INCORRECT: "Network access control list (ACL)" is incorrect. Although Network ACLs are virtual firewalls which control access within a VPC, Network ACLs exist on the subnet level, not on the instance level.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

✓ Which of the following statements is INCORRECT regarding Amazon EBS Elastic Volumes? *1/1

- ○ Amazon EBS Elastic Volumes can persist data after their termination
- ◉ Amazon EBS Elastic Volumes can be bound to several Availability Zones (AZs) ✓
- ○ Amazon EBS Elastic Volumes can be mounted to one instance at a time
- ○ Amazon EBS Elastic Volumes are bound to a specific Availability Zone (AZ)

Feedback

Explanation
Correct option:

Amazon EBS Elastic Volumes can be bound to several Availability Zones (AZs)

An Amazon EBS Elastic Volume is a durable, block-level storage device that you can attach to your instances. After you attach a volume to an instance, you can use it as you would use a physical hard drive.

When using Amazon EBS Elastic Volumes, the volume, and the instance must be in the same Availability Zone (AZ).

Incorrect options:

Amazon EBS Elastic Volumes can be mounted to one instance at a time - At the Certified Cloud Practitioner level, Amazon EBS Elastic Volumes can be mounted to one instance at a time. It is also possible that an Amazon EBS Elastic Volume is not mounted to an instance.

Amazon EBS Elastic Volumes are bound to a specific Availability Zone (AZ) - As mentioned, when using Amazon EBS Elastic Volumes, the volume and the instance must be in the same Availability Zone(AZ).

Amazon EBS Elastic Volumes can persist data after their termination - Unlike an Amazon EC2 instance store, an Amazon EBS Elastic Volume is off-instance storage that can persist independently from the life of an instance.

Reference:

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

✓ Which combination of steps will enable multi-factor authentication (MFA) on an AWS account? (Select TWO.) *1/1

- [ ] Activate the MFA device by using Amazon GuardDuty.
- [x] Activate the MFA device in the IAM console or by using the AWS CLI. ✓
- [ ] Activate AWS Shield on an MFA-compatible device.
- [x] Acquire an MFA-compatible device. ✓
- [ ] Contact AWS Support to initiate MFA activation.

Feedback

Explanation
Multi-factor authentication (MFA) in AWS is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS Management Console, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have).

Taken together, these multiple factors provide increased security for your AWS account settings and resources. You can enable MFA for your AWS account and for individual IAM users you have created under your account. MFA can also be used to control access to AWS service APIs.

You will first need a device capable of providing an application which can support virtual MFA. There are several form factors to choose from:

Once you have this device, you will need to register it to your AWS account through the AWS Identity and Access Management (IAM) service.

CORRECT: "Acquire an MFA-compatible device" is a correct answer (as explained above.)

CORRECT: "Activate the MFA device in the IAM console or by using the AWS CLI" is also a correct answer (as explained above.)

INCORRECT: "Contact AWS Support to initiate MFA activation" is incorrect. AWS Support cannot enable MFA for you regardless of which support tier you are using.

INCORRECT: "Activate AWS Shield on an MFA-compatible device" is incorrect. AWS Shield is a DDoS mitigation service and has nothing to do with MFA.

INCORRECT: "Activate the MFA device by using Amazon GuardDuty" is incorrect. Amazon GuardDuty is an intelligent threat detection service which has nothing to do with MFA.

References:

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

✓ Which of the following must be used together to gain programmatic access to an AWS account? (Select TWO.) *1/1

- [x] An access key ID ✓
- [ ] A secondary key
- [x] A secret access key ✓
- [ ] A primary key
- [ ] A user ID

Feedback

Explanation
Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY).

Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

CORRECT: "An access key ID" is the correct answer.

CORRECT: "A secret access key" is the correct answer.

INCORRECT: "A primary key" is incorrect. Primary keys are not associated with authentication.

INCORRECT: "A user ID" is incorrect. A user ID is used to logon using the AWS Management Console, not programmatically.

INCORRECT: "A secondary key" is incorrect. Secondary keys are not associated with authentication.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

✓ Who is responsible for configuration management under the AWS shared responsibility model? *1/1

- ○ It is solely the responsibility of the customer.
- ○ It is solely the responsibility of AWS.
- ◉ It is shared between AWS and the customer. ✓
- ○ It is not part of the AWS shared responsibility model.

Feedback

AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

✓ Which of the following statements are true about AWS Regions and Availability Zones (AZ)? (Select two) *1/1

- [x] All traffic between Availability Zones (AZ) is encrypted ✓
- [ ] An Availability Zone (AZ) is a physical location where AWS clusters the data centers
- [ ] AWS calls each group of logical data centers as AWS Regions
- [ ] Traffic between Availability Zones (AZ) is not encrypted by default, but can be configured from AWS console
- [x] Each AWS Region consists of multiple, isolated, and physically separate Availability Zones (AZ) within a geographic area ✓

Feedback

Explanation
Correct options:

Each AWS Region consists of multiple, isolated, and physically separate Availability Zones (AZ) within a geographic area

AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. AWS calls each group of logical data centers an Availability Zone (AZ). Each AWS Region consists of multiple, isolated, and physically separate Availability Zones (AZ) within a geographic area.

Each Availability Zone (AZ) has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple Availability Zones (AZ) to achieve even greater fault tolerance. AWS infrastructure Regions meet the highest levels of security, compliance, and data protection.

All traffic between Availability Zones (AZ) is encrypted

All Availability Zones (AZ) in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber providing high-throughput, low-latency networking between Availability Zones (AZ). All traffic between Availability Zones (AZ) is encrypted.

Incorrect options:

Traffic between Availability Zones (AZ) is not encrypted by default, but can be configured from AWS console - All traffic between Availability Zones (AZ) is encrypted.

An Availability Zone (AZ) is a physical location where AWS clusters the data centers - AWS has the concept of a Region, which is a physical location around the world where AWS clusters the data centers.

AWS calls each group of logical data centers as AWS Regions - AWS has the concept of a Region, which is a physical location around the world where AWS clusters the data centers. AWS calls each group of logical data centers as an Availability Zone (AZ).

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

✓ In AWS IAM, what are the characteristics of users and groups? (Select TWO.) *1/1

- [x] A user can be a member of multiple groups. ✓
- [ ] All new users are automatically added to a default group.
- [ ] Groups can be nested and can contain other groups.
- [ ] A user can only be a member of a single group at one time.
- [x] Groups can contain users only and cannot be nested. ✓

Feedback

Explanation
In IAM, a user can be a member of multiple groups. One IAM user can be a part of a maximum of 5 groups. Also Groups are a flat hierarchy of users with similar permissions, and you cannot place a group within another group.

CORRECT: "A user can be a member of multiple groups" is the correct answer (as explained above.)

CORRECT: "Groups can contain users only and cannot be nested" is also a correct answer (as explained above.)

INCORRECT: "Groups can be nested and can contain other groups" is incorrect. This is also explained above.

INCORRECT: "A user can only be a member of a single group at one time" is incorrect. A user group can contain many users, and a user can belong to multiple user groups.

INCORRECT: "All new users are automatically added to a default group" is incorrect. Users do not have to be added to any group and can exist simply as users.

References:

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

✓ As part of a flexible pricing model, AWS offers two types of Savings Plans. Which of the following are the Savings Plans from AWS? *1/1

- ○ Compute Savings Plans, Storage Savings Plans
- ○ Instance Savings Plans, Storage Savings Plans
- ◉ Compute Savings Plans, EC2 Instance Savings Plans ✓
- ○ Reserved Instances (RI) Savings Plans, EC2 Instance Savings Plans Explanation

Feedback

Explanation
Correct option:

Compute Savings Plans, EC2 Instance Savings Plans

Savings Plans is a flexible pricing model that provides savings of up to 72% on your AWS compute usage. This pricing model offers lower prices on Amazon EC2 instances usage, regardless of instance family, size, OS, tenancy or AWS Region, and also applies to AWS Fargate and AWS Lambda usage.

Savings Plans offer significant savings over On-Demand, just like EC2 Reserved Instances, in exchange for a commitment to use a specific amount of compute power (measured in $/hour) for a one or three-year period. You can sign up for Savings Plans for a 1- or 3-year term and easily manage your plans by taking advantage of recommendations, performance reporting and budget alerts in the AWS Cost Explorer.

AWS offers two types of Savings Plans:

Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage. For example, with Compute Savings Plans, you can change from C4 to M5 instances, shift a workload from EU (Ireland) to EU (London), or move a workload from EC2 to Fargate or Lambda at any time and automatically continue to pay the Savings Plans price.

EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% in exchange for a commitment to the usage of individual instance families in a region (e.g. M5 usage in N. Virginia). This automatically reduces your cost on the selected instance family in that region regardless of AZ, size, OS or tenancy. EC2 Instance Savings Plans give you the flexibility to change your usage between instances within a family in that region. For example, you can move from c5.xlarge running Windows to c5.2xlarge running Linux and automatically benefit from the Savings Plans prices.

How Savings Plans Work: via - https://aws.amazon.com/savingsplans/

Incorrect options:

Compute Savings Plans, Storage Savings Plans

Reserved Instances (RI) Savings Plans, EC2 Instance Savings Plans

Instance Savings Plans, Storage Savings Plans

These three options contradict the explanation above, so these options are incorrect.

References:

https://aws.amazon.com/savingsplans/

https://aws.amazon.com/savingsplans/faq/

✓ Which cloud architecture design principle is supported by deploying workloads across multiple Availability Zones? *1/1

- ○ Automate infrastructure.
- ○ Enable elasticity.
- ○ Design for agility.
- ◉ Design for failure. ✓

Feedback

Explanation
Amazon EC2 instances can be deployed in an Amazon VPC across multiple Availability Zones. You would then typically use an Elastic Load Balancer (ELB) to distribute load between the available instances. This architecture enables high availability as if a single instance fails or if something fails that causes an outage in an entire Availability Zone, the application still has available instances to continue to service demand.

CORRECT: "Design for failure" is the correct answer.

INCORRECT: "Design for agility" is incorrect. This is not an example of agility; it is an example of high availability and fault tolerance.

INCORRECT: "Automate infrastructure" is incorrect. This is not an example of automating.

INCORRECT: "Enable elasticity" is incorrect. This is not an example of elasticity. Elasticity would be enabled by using Amazon EC2 Auto Scaling.

References:

https://aws.amazon.com/architecture/well-architected/

✓ Which service can be used to manage configuration versions? * 1/1

- (●) AWS Config ✓
- ( ) Amazon Inspector
- ( ) AWS Artifact
- ( ) AWS Service Catalog

Feedback

Explanation
AWS Config is a fully-managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and regulatory compliance.

CORRECT: "AWS Config" is the correct answer.

INCORRECT: "AWS Service Catalog" is incorrect. AWS Service Catalog is used to create and manage catalogs of IT services that you have approved for use on AWS, including virtual machine images, servers, software, and databases to complete multi-tier application architectures.

INCORRECT: "AWS Artifact" is incorrect. AWS Artifact is a central resource for compliance-related information. This service can be used to get compliance information related to AWS' certifications/attestations.

INCORRECT: "Amazon Inspector" is incorrect. Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

References:

https://docs.aws.amazon.com/config/latest/developerguide/how-does-config-work.html

✓ A financial services company needs to retain its data for 10 years to meet compliance norms. Which Amazon Simple Storage Service (Amazon S3) storage class is the best fit for this use case considering that the data has to be stored at a minimal cost? *1/1

- ○ Amazon S3 Intelligent-Tiering
- ○ Amazon S3 Glacier Flexible Retrieval
- ◉ Amazon S3 Glacier Deep Archive ✓
- ○ Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

Feedback

Explanation
Correct option:

Amazon S3 Glacier Deep Archive

Amazon S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases, and is a cost-effective and easy-to-manage alternative to magnetic tape systems, whether they are on-premises libraries or off-premises services.

Amazon S3 Glacier Deep Archive complements Amazon S3 Glacier, which is ideal for archives where data is regularly retrieved and some of the data may be needed in minutes. All objects stored in S3 Glacier Deep Archive are replicated and stored across at least three geographically-dispersed Availability Zones, protected by 99.999999999% of durability, and can be restored within 12 hours.

Incorrect options:

Amazon S3 Glacier Flexible Retrieval - Amazon S3 Glacier Flexible Retrieval delivers low-cost storage, up to 10% lower cost (than Amazon S3 Glacier Instant Retrieval), for archive data that is accessed 1—2 times per year and is retrieved asynchronously. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases, Amazon S3 Glacier Flexible Retrieval (formerly Amazon S3 Glacier) is the ideal storage class.

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) - Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files. S3 Storage Classes can be configured at the object level and a single bucket can contain objects stored across S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can also use S3 Lifecycle policies to automatically transition objects

between storage classes without any application changes.

Amazon S3 Intelligent-Tiering - Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is the only cloud storage class that delivers automatic cost savings by moving objects between four access tiers when access patterns change. The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without operational overhead. It works by storing objects in four access tiers: two low latency access tiers optimized for frequent and infrequent access, and two optional archive access tiers designed for asynchronous access that are optimized for rare access.

Reference:

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

✗ Which of the following statements are true about AWS Shared Responsibility Model? (Select two) *0/1

- [ ] AWS trains AWS employees, but a customer must train their own employees
- [x] AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications ✓
- [x] For abstracted services, such as Amazon S3, AWS operates the infrastructure layer, the operating system, platforms, encryption options, and appropriate permissions for accessing the S3 resources ✗
- [ ] Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and hence AWS will perform all of the necessary security configuration and management tasks
- [ ] AWS maintains the configuration of its infrastructure devices and is responsible for configuring the guest operating systems, databases, and applications

Correct answer

- [x] AWS trains AWS employees, but a customer must train their own employees
- [x] AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications

Feedback

Explanation
Correct options:

AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest Operating system and applications

AWS trains AWS employees, but a customer must train their own employees

"Security of the Cloud" is the responsibility of AWS - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. As part of Patch Management, a Shared Control responsibility of AWS Shared Responsibility Model, AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

"Security in the Cloud" is the responsibility of the customer. Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.

As part of Awareness & Training, a Shared Control responsibility of the AWS Shared Responsibility Model, AWS trains AWS employees, but a customer must train their own

employees.

AWS Shared Responsibility Model: via - https://aws.amazon.com/compliance/shared-responsibility-model/

Incorrect options:

AWS maintains the configuration of its infrastructure devices and is responsible for configuring the guest operating systems, databases, and applications - As part of Configuration Management, a Shared Control responsibility of the AWS Shared Responsibility Model, AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and hence AWS will perform all of the necessary security configuration and management tasks - A service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for the management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

For abstracted services, such as Amazon S3, AWS operates the infrastructure layer, the operating system, platforms, encryption options, and appropriate permissions for accessing the S3 resources - For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

Reference:

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

✓ Which component of the AWS global infrastructure is made up of one or more discrete data centers that have redundant power, networking, and connectivity? *1/1

- ○ AWS Region
- ◉ Availability Zone ✓
- ○ Edge location
- ○ AWS Outposts

Feedback

An Availability Zone (AZ) is a component of the AWS global infrastructure that is made up of one or more discrete data centers that have redundant power, networking, and connectivity. Each AZ is physically separated from other AZs within a region, and is designed to be fault-tolerant and provide low-latency networking.

✓ Which AWS service lets connected devices easily and securely interact with cloud applications and other devices? *1/1

- ( ) Amazon Workspaces
- (•) AWS IoT Core ✓
- ( ) AWS Directory Service
- ( ) AWS Server Migration Service (SMS)

Feedback

Explanation
AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely.

CORRECT: "AWS IoT Core" is the correct answer.

INCORRECT: "AWS Directory Service" is incorrect. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud

INCORRECT: "Amazon Workspaces" is incorrect. Amazon WorkSpaces is a managed, secure cloud desktop service

INCORRECT: "AWS Server Migration Service (SMS)" is incorrect. AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for you to migrate thousands of on-premises workloads to AWS.

References:

https://aws.amazon.com/iot-core/

✓ What can a Cloud Practitioner use the AWS Total Cost of Ownership (TCO) Calculator for? *1/1

- ○ Enable billing alerts to monitor actual AWS costs compared to estimated costs
- ◉ Estimate savings when comparing the AWS Cloud to an on-premises environment ✓
- ○ Estimate a monthly bill for the AWS Cloud resources that will be used
- ○ Generate reports that break down AWS Cloud compute costs by duration, resource, or tags

Feedback

Explanation
The TCO calculators allow you to estimate the cost savings when using AWS, compared to on-premises, and provide a detailed set of reports that can be used in executive presentations. The calculators also give you the option to modify assumptions that best meet your business needs.

CORRECT: "Estimate savings when comparing the AWS Cloud to an on-premises environment" is the correct answer.

INCORRECT: "Generate reports that break down AWS Cloud compute costs by duration, resource, or tags" is incorrect. This describes the AWS Cost & Usage Report.

INCORRECT: "Estimate a monthly bill for the AWS Cloud resources that will be used" is incorrect. This describes the AWS Pricing Calculator (or Simple Monthly Calculator).

INCORRECT: "Enable billing alerts to monitor actual AWS costs compared to estimated costs" is incorrect. Billing alerts can be enabled using Amazon CloudWatch.

References:

https://aws.amazon.com/tco-calculator/

✓ Which of the following will help you control the incoming traffic to an Amazon EC2 instance? *1/1

- ○ AWS Resource Group
- ○ Route Table
- ○ Network access control list (network ACL)
- ◉ Security Group ✓

Feedback

Correct option:
Security Group

A security group acts as a virtual firewall for your Amazon EC2 instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance. When you launch an instance, you can specify one or more security groups. If you don't specify a security group, Amazon EC2 uses the default security group. You can add rules to each security group that allows traffic to or from its associated instances. You can modify the rules for a security group at any time. New and modified rules are automatically applied to all instances that are associated with the security group. When Amazon EC2 decides whether to allow traffic to reach an instance, it evaluates all of the rules from all of the security groups that are associated with the instance. Security is a shared responsibility between AWS and you. AWS provides security groups as one of the tools for securing your instances, and you need to configure them to meet your security needs. If you have requirements that aren't fully met by security groups, you can maintain your own firewall on any of your instances in addition to using security groups.

Incorrect options:
AWS Resource Group - You can use AWS Resource Groups to organize your AWS resources. Resource groups make it easier to manage and automate tasks on large numbers of resources at one time. Resource Groups feature permissions are at the account level. As long as users who are sharing your account have the correct IAM permissions, they can work with the resource groups that you create. Resource Groups are for grouping resources for managing the resources. They do not provide access to Amazon EC2 instances.

Network access control list (network ACL) - A Network access control list (network ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Route Table - A Route table contains a set of rules, called routes, that are used to determine where network traffic from your VPC is directed. You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. Each route in a route table specifies the range of IP addresses where you want the traffic to go (the destination) and the gateway, network interface, or connection through which to send the traffic (the target).
References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-

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

✓ AWS Support plans are designed to give the right mix of tools and access to expertise for successfully running a business using AWS. *1/1

Which support plan(s) offers the full set of checks for AWS Trusted Advisor best practices and also provides support for programmatic case management?

- ○ Only AWS Enterprise Support plan
- ○ AWS Developer Support, AWS Business Support and AWS Enterprise Support plans
- ○ AWS Enterprise On-Ramp Support plan after paying an additional fee and AWS Enterprise Support plan
- ◉ AWS Business Support, AWS Enterprise On-Ramp, and AWS Enterprise Support plans ✓

Feedback

Explanation
Correct option:

AWS Business Support, AWS Enterprise On-Ramp, and AWS Enterprise Support plans

AWS Trusted Advisor provides you with real-time guidance to help you provision your resources following AWS best practices.

The full set of AWS Trusted Advisor checks are included with Business and Enterprise Support plans. These checks can help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits.

AWS Support API provides programmatic access to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status. AWS Support API is available for Business, Enterprise On-Ramp and Enterprise Support plans.

Comparing AWS Support Plans: via - https://aws.amazon.com/premiumsupport/plans/

Incorrect options:

Only AWS Enterprise Support plan

AWS Developer Support, AWS Business Support and AWS Enterprise Support plans

AWS Enterprise On-Ramp Support plan after paying an additional fee and AWS Enterprise Support plan

These three options contradict the explanation provided above, so these options are incorrect.

Reference:

https://aws.amazon.com/premiumsupport/plans/

✓ Which of the following AWS services will help provision a logically isolated network for your AWS resources? *1/1

- (●) Amazon Virtual Private Cloud (Amazon VPC) ✓
- ( ) AWS PrivateLink
- ( ) Amazon Route 53
- ( ) AWS Firewall Manager

Feedback

Explanation
Correct option:

Amazon Virtual Private Cloud (Amazon VPC)

Amazon Virtual Private Cloud (Amazon VPC) is a service that lets you launch AWS resources in a logically isolated virtual network that you define. You have complete control over your virtual networking environment, including the selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 for most resources in your virtual private cloud, helping to ensure secure and easy access to resources and applications.

As one of AWS's foundational services, Amazon VPC makes it easy to customize your VPC's network configuration. You can create a public-facing subnet for your web servers that have access to the internet. It also lets you place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. Amazon VPC lets you use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Incorrect options:

AWS PrivateLink - AWS PrivateLink provides private connectivity between Amazon VPCs and services hosted on AWS or on-premises, securely on the Amazon network. By providing a private endpoint to access your services, AWS PrivateLink ensures your traffic is not exposed to the public internet.

Amazon Route 53 - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.

AWS Firewall Manager - AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations. As new applications are created, Firewall Manager makes it easy to bring new applications and resources into compliance by enforcing a common set of security rules.

Reference:

https://aws.amazon.com/vpc/

✓ Which of the following statements are true about AWS Elastic Beanstalk? (Select two) *1/1

- [x] With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications ✓
- [ ] AWS Elastic Beanstalk supports web applications built on different languages. But, AWS Elastic Beanstalk cannot be used for deploying non-web applications
- [ ] AWS Elastic Beanstalk supports Java, .NET, PHP, but does not support Docker web applications
- [ ] AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, and application deployment, creating an environment that runs a version of your application. However, auto-scaling functionality cannot be automated using AWS Elastic Beanstalk
- [x] There is no additional charge for AWS Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes ✓

Feedback

Explanation
Correct options:

With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications

There is no additional charge for AWS Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes

With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and AWS Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

AWS Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby. When you deploy your application, AWS Elastic Beanstalk builds the selected supported platform version and provisions one or more AWS resources, such as Amazon EC2 instances, to run your application.

There is no additional charge for AWS Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes.

Incorrect options:

AWS Elastic Beanstalk supports Java, .NET, PHP, but does not support Docker web applications - AWS Elastic Beanstalk supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker web applications.

AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, and

application deployment, creating an environment that runs a version of your application. However, auto-scaling functionality cannot be automated using AWS Elastic Beanstalk - AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, auto-scaling, and application deployment, creating an environment that runs a version of your application. You can simply upload your deployable code (e.g., WAR file), and AWS Elastic Beanstalk does the rest.

AWS Elastic Beanstalk supports web applications built on different languages. But, AWS Elastic Beanstalk cannot be used for deploying non-web applications - AWS Elastic Beanstalk supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker, and is ideal for web applications. However, due to Elastic Beanstalk's open architecture, non-web applications can also be deployed using Elastic Beanstalk.

References:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html

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

✓ A multinational company has just moved its infrastructure to AWS Cloud and has employees traveling to different offices around the world. How should the company set the AWS accounts? *1/1

- ○ As employees travel, they can use other employees' accounts
- ○ Create global permissions so users can access resources from all around the world
- ◉ There is nothing to do, AWS Identity and Access Management (AWS IAM) is a global service ✓
- ○ Create an IAM user for each user in each AWS region

Feedback

Explanation
Correct option:

There is nothing to do, AWS Identity and Access Management (AWS IAM) is a global service

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

AWS IAM is a global service. Users created within IAM can access their accounts all around the world, and deploy resources in every region.

Incorrect options:

Create an IAM user for each user in each AWS region - IAM users can access their accounts from different AWS regions.

Create global permissions so users can access resources from all around the world - AWS Identity and Access Management (AWS IAM) is a global service. You can use it globally without implementing anything.

As employees travel, they can use other employees' accounts - You should never share you IAM user credentials.

Reference:

https://aws.amazon.com/iam/

✓ A company using a hybrid cloud would like to store secondary backup copies of the on-premises data. Which Amazon S3 Storage Class would you use for a cost-optimal yet rapid access solution? *1/1

- Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
- Amazon S3 Standard
- Amazon S3 Glacier Deep Archive
- Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) ✓

Feedback

Explanation
Correct option:

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single Availability Zone (AZ) and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. It's a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 cross-region replication (S3 CRR).

Exam Alert:

Please review this detailed comparison of S3 Storage Classes as you can expect a few questions on this aspect of S3: via - https://aws.amazon.com/s3/storage-classes/

Incorrect options:

Amazon S3 Glacier Deep Archive - Amazon S3 Glacier Deep Archive storage class is designed to provide durable and secure long-term storage for large amounts of data at a price that is competitive with off-premises tape archival services. Data is stored across 3 or more AWS Availability Zones(AZs) and can be retrieved in 12 hours or less. You no longer need to deal with expensive and finicky tape drives, arrange for off-premises storage, or worry about migrating data to newer generations of media.

Amazon S3 Standard - Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, Amazon S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) - Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB

retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files. It can be used for backups, but it is more expensive than S3 One Zone - Infrequent Access. Hence, S3 One Zone - Infrequent Access is a better option for secondary backup copies.

Reference:

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

✓ What AWS service offers managed DDoS protection? * 1/1

- ○ AWS Firewall Manager
- ○ Amazon Inspector
- ◉ AWS Shield ✓
- ○ Amazon GuardDuty

Feedback

Explanation
AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.

CORRECT: "AWS Shield" is the correct answer (as explained above.)

INCORRECT: "AWS Firewall Manager" is incorrect. AWS Firewall Manager is a security management service which allows you to centrally configure and manage firewall rules across your accounts and does not protect from DDoS attacks.

INCORRECT: "Amazon GuardDuty" is incorrect. Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation. It does not protect you from DDoS attacks.

INCORRECT: "Amazon Inspector" is incorrect also as Inspector is a fully managed vulnerability assessment tool and does not protect from DDoS attacks.

References:

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

Google Forms