Question 1
Which of the following are correct statements regarding the AWS Global Infrastructure? (Select two)

1] Each Availability Zone (AZ) consists of one or more discrete data centers
2] Each AWS Region consists of a minimum of two Availability Zones (AZ)
3] Each AWS Region consists of a minimum of three Availability Zones (AZ)
4] Each AWS Region consists of two or more Edge Locations
5] Each Availability Zone (AZ) consists of two or more discrete data centers

Overall explanation
Correct options:

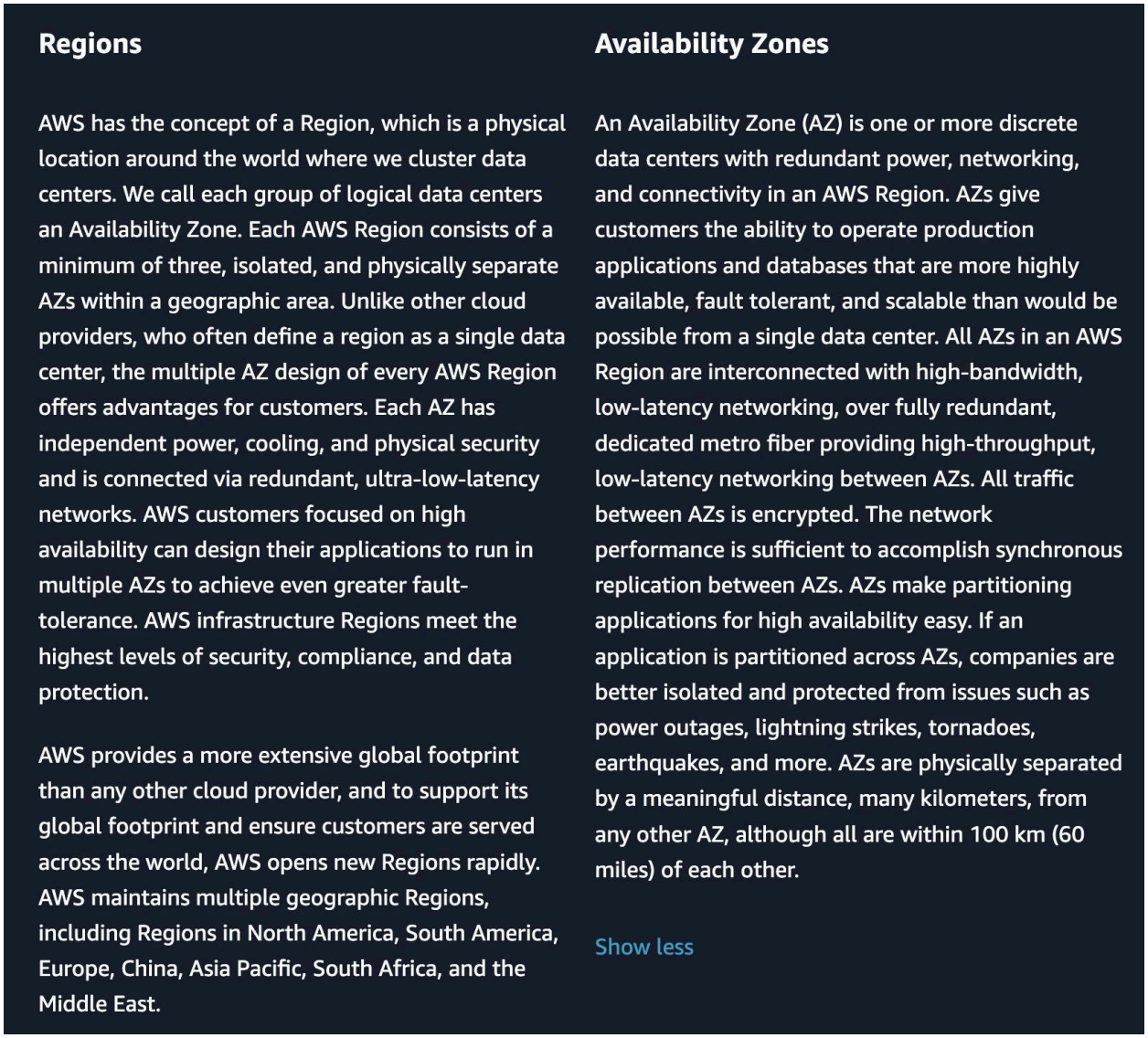
Each AWS Region consists of a minimum of three Availability Zones (AZ)

Each Availability Zone (AZ) consists of one or more discrete data centers

AWS has the concept of a Region, which is a physical location around the world where AWS clusters its data centers. AWS calls each group of logical data centers an Availability Zone (AZ). Each AWS Region consists of a minimum of three, isolated, and physically separate AZs within a geographic area. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks.

An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. All AZs 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 AZs.

AWS Regions and Availability Zones Overview:



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

Incorrect options:

Each AWS Region consists of a minimum of two Availability Zones (AZ)

Each Availability Zone (AZ) consists of two or more discrete data centers

Each AWS Region consists of two or more Edge Locations

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

Reference:

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

Domain
Technology

Question 2
Which of the following are the advantages of cloud computing? (Select three)
1] Trade capital expense for variable expense
2] Trade variable expense for capital expense
3] Spend money on building and maintaining data centers
4] Allocate a few months of planning for your infrastructure capacity needs
5] Go global in minutes and deploy applications in multiple regions around the world with just a few clicks
6] Benefit from massive economies of scale

Overall explanation
Correct options:

Benefit from massive economies of scale

Trade capital expense for variable expense

Go global in minutes and deploy applications in multiple regions around the world with just a few clicks

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:

Spend money on building and maintaining data centers - With cloud computing, you can focus on projects that differentiate your business, not the infrastructure. You don't need to spend money on building and maintaining data centers as the Cloud provider takes care of that.

Allocate a few months of planning for your infrastructure capacity needs - With cloud computing, you don't need to guess on your infrastructure capacity needs. 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. There is no need to allocate a few months of infrastructure planning.

Trade variable expense for capital expense - With cloud computing, you actually trade capital expense for variable expense.

Question 3

Which of the following statements are CORRECT regarding the Availability Zone (AZ) specific characteristics of Amazon Elastic Block Store (EBS) and Amazon Elastic File System (Amazon EFS) storage types?

1] EBS volume can be attached to one or more instances in multiple Availability Zones (AZ) and EFS file system can be mounted on instances across multiple Availability Zones (AZ)

2] EBS volume can be attached to one or more instances in multiple Availability Zones (AZ) and EFS file system can be mounted on instances in the same Availability Zone (AZ)

3] EBS volume can be attached to a single instance in the same Availability Zone (AZ) whereas EFS file system can be mounted on instances across multiple Availability Zones (AZ)

4] EBS volume can be attached to a single instance in the same Availability Zone (AZ) and EFS file system can only be mounted on instances in the same Availability Zone (AZ)

Overall explanation
Correct option:

EBS volume can be attached to a single instance in the same Availability Zone (AZ) whereas EFS file system can be mounted on instances across multiple Availability Zones (AZ)

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

The service is designed to be highly scalable, highly available, and highly durable. Amazon EFS file systems store data and metadata across multiple Availability Zones (AZ) in an AWS Region. EFS file system can be mounted on instances across multiple Availability Zones (AZ).

Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale.

Designed for mission-critical systems, EBS volumes are replicated within an Availability Zone (AZ) and can easily scale to petabytes of data. You can attach an available EBS volume to one instance that is in the same Availability Zone (AZ) as the volume.

Incorrect options:

EBS volume can be attached to one or more instances in multiple Availability Zones (AZ) and EFS file system can be mounted on instances in the same Availability Zone (AZ)

EBS volume can be attached to a single instance in the same Availability Zone (AZ) and EFS file system can only be mounted on instances in the same Availability Zone (AZ)

EBS volume can be attached to one or more instances in multiple Availability Zones (AZ) and EFS file system can be mounted on instances across multiple Availability Zones (AZ)

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

References:

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

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

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

Domain
Technology

Question 4
Which tool/service will help you access AWS services using programming language-specific APIs?

1] AWS Management Console
2] Integrated Development Environments (IDE)
3] AWS Command Line Interface (CLI)
4] AWS Software Developer Kit (SDK)

Overall explanation
Correct option:

AWS Software Developer Kit (SDK)

SDKs take the complexity out of coding by providing language-specific APIs for AWS services. For example, the AWS SDK for JavaScript simplifies the use of AWS Services by providing a set of libraries that are consistent and familiar for JavaScript developers. It provides support for API lifecycle considerations such as credential management, retries, data marshaling, serialization, and deserialization. AWS SDKs are offered in several programming languages to make it simple for developers working on different

programming and scripting languages. So, AWS SDK can help with using AWS services from within an application using language-specific APIs.

Incorrect options:

AWS Management Console - The AWS Management Console is a web application that comprises and refers to a broad collection of service consoles for managing Amazon Web Services. When you first sign in, you see the console home page. The home page provides access to each service console as well as an intuitive user interface for exploring AWS and getting helpful tips.

AWS Command Line Interface (CLI) - The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts. CLI cannot be used with language-specific APIs.

Integrated Development Environments (IDE) - An integrated development environment (IDE) provides a set of coding productivity tools such as a source code editor, a debugger, and build tools. Cloud9 IDE is an offering from AWS under IDEs.

References:

https://aws.amazon.com/tools/

https://aws.amazon.com/cli/

Domain
Technology

Question 5
A research group wants to use EC2 instances to run a scientific computation application that has a fault tolerant architecture. The application needs high-performance hardware disks that provide fast I/O performance. As a Cloud Practitioner, which of the following storage options would you recommend as the MOST cost-effective solution?

1] Instance Store
2] Amazon Elastic File System (Amazon EFS)
3] Amazon Simple Storage Service (Amazon S3)
4] Amazon Elastic Block Store (EBS)

Overall explanation
Correct option:

Instance Store

An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. This is a good option when you need storage with very low latency, but you don't need the data to persist when the instance terminates or you can take advantage of fault-tolerant architectures. For this use-case, the computation application itself has a fault tolerant architecture, so it can automatically handle any failures of Instance Store volumes.

As the Instance Store volumes are included as part of the instance's usage cost, therefore this is the correct option.

EC2 Instances Store Overview:

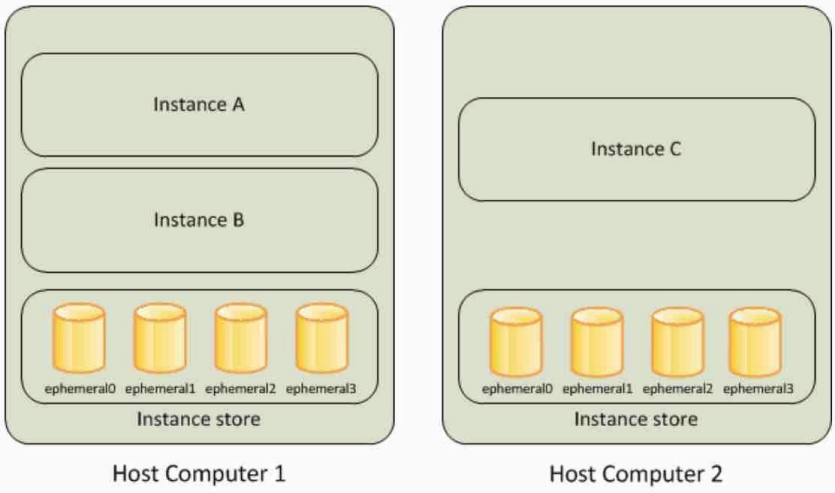
Amazon EC2 Instance Store

PDF | Kindle | RSS

An *instance store* provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.

An instance store consists of one or more instance store volumes exposed as block devices. The size of an instance store as well as the number of devices available varies by instance type.

The virtual devices for instance store volumes are `ephemeral[0-23]`. Instance types that support one instance store volume have `ephemeral0`. Instance types that support two instance store volumes have `ephemeral0` and `ephemeral1`, and so on.



via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

Incorrect options:

Amazon Elastic File System (Amazon EFS) - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS file system. EFS is not available as a hardware disk on the instance, so this option is not correct.

Amazon Elastic Block Store (EBS) - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. EBS is not available as a hardware disk on the instance, so this option is not correct.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 is not available as a hardware disk on the instance, so this option is not correct.

Reference:

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

Domain
Technology

Question 6
Which of the following are the storage services offered by the AWS Cloud? (Select two)

1] Amazon Simple Storage Service (Amazon S3)
2] Amazon Simple Notification Service (SNS)
3] Amazon Simple Queue Service (SQS)
4] Amazon Elastic Compute Cloud (Amazon EC2)
5] Amazon Elastic File System (Amazon EFS)

Overall explanation
Correct options:

Amazon Simple Storage Service (Amazon S3)

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Amazon Elastic File System (Amazon EFS)

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

Incorrect options:

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the AWS cloud. You can use EC2 to provision virtual servers on AWS Cloud.

Amazon Simple Queue Service (SQS) - Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

Amazon Simple Notification Service (SNS) - Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Using Amazon SNS topics, your publisher systems can fan-out messages to a large number of subscriber endpoints for parallel processing, including Amazon SQS queues, AWS Lambda functions, and HTTP/S webhooks. Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

References:

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

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

Domain
Technology

Question 7
A multi-national corporation wants to get expert professional advice on migrating to AWS and managing their applications on AWS Cloud. Which of the following entities would you recommend for this engagement?

1]Concierge Support Team
2] APN Consulting Partner
3]AWS Trusted Advisor
4] APN Technology Partner
5] Overall explanation

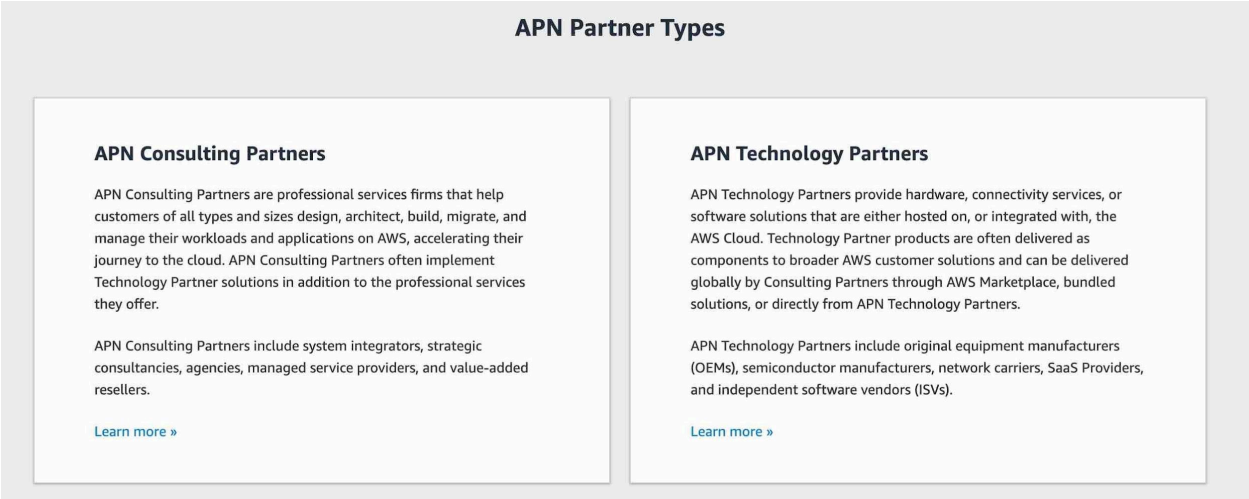
Correct option:

APN Consulting Partner

The AWS Partner Network (APN) is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers.

APN Consulting Partners are professional services firms that help customers of all types and sizes design, architect, build, migrate, and manage their workloads and applications on AWS, accelerating their migration to AWS cloud.

APN Partner Types Overview:



via - https://aws.amazon.com/partners/

Incorrect options:

APN Technology Partner - APN Technology Partners provide hardware, connectivity services, or software solutions that are either hosted on or integrated with, the AWS Cloud. APN Technology Partners cannot help in migrating to AWS and managing applications on AWS Cloud.

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 on cost optimization, security, fault tolerance, service limits, and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing

improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. All AWS customers get access to the seven core Trusted Advisor checks to help increase the security and performance of the AWS environment. Trusted Advisor cannot be used to migrate to AWS and manage applications on AWS Cloud.

Concierge Support Team - The Concierge Support Team are AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries. The Concierge Support Team is only available for the Enterprise Support plan. Concierge Support Team cannot help in migrating to AWS and managing applications on AWS Cloud.

Reference:

https://aws.amazon.com/partners/

Domain
Cloud Concepts

Question 8
A company wants to have control over creating and using its own keys for encryption on AWS services. Which of the following can be used for this use-case?
1] AWS Secrets Manager
2] customer managed key (CMK)
3] AWS managed key
4] AWS owned key

Overall explanation
Correct option:

customer managed key (CMK)

An AWS KMS key is a logical representation of a cryptographic key. A KMS key contains metadata, such as the key ID, key spec, key usage, creation date, description, and key state. Most importantly, it contains a reference to the key material that is used when you perform cryptographic operations with the KMS key.

The 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.

Incorrect options:

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. You cannot use AWS Secrets Manager for creating and using your own keys for encryption on AWS services.

AWS managed key - AWS managed keys are KMS keys in your account that are created, managed, and used on your behalf by an AWS service integrated with AWS KMS.

AWS owned key - AWS owned keys are a collection of KMS keys that an AWS service owns and manages for use in multiple AWS accounts. Although AWS owned keys are not in your AWS account, an AWS service can use an AWS owned key to protect the resources in your account.

Reference:

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

Domain
Security and Compliance

Question 9 **Correct**

According to the AWS Shared Responsibility Model, which of the following are responsibilities of AWS? (Select two)

1] Enabling Multi Factor Authentication on AWS accounts in your organization
2] Creating IAM role for accessing Amazon EC2 instances
3] Creating S3 bucket policies for appropriate user access
4] Replacing faulty hardware of Amazon EC2 instances

5] Operating the infrastructure layer, the operating system and the platform for the Amazon S3 service

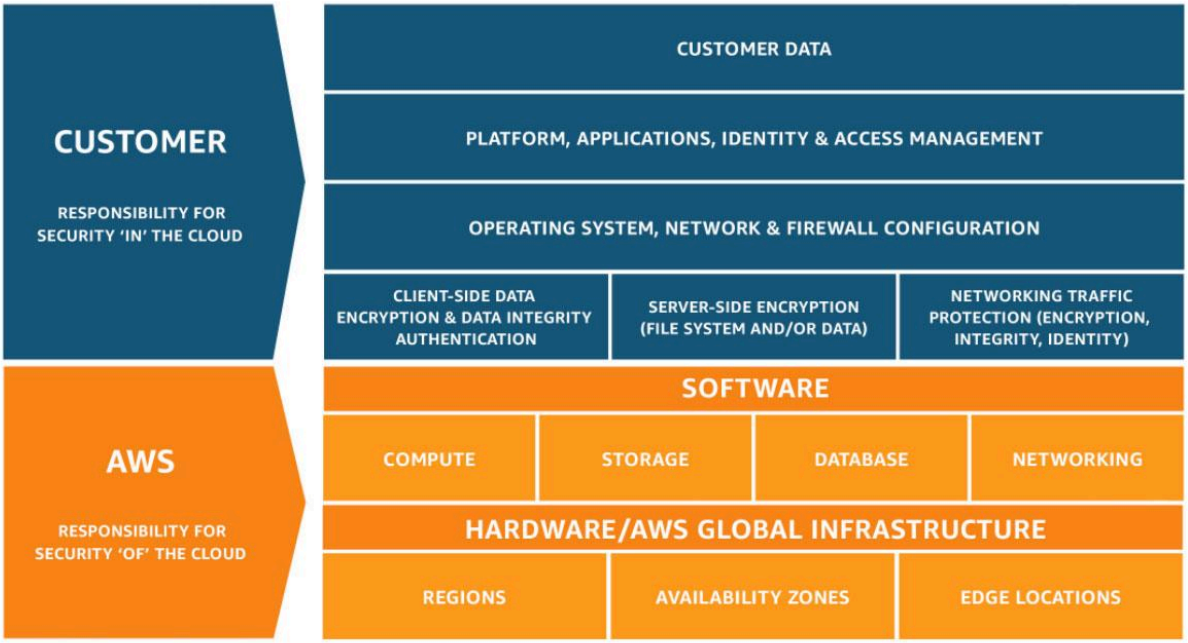
Overall explanation
Correct options:

According to the AWS Shared Responsibility Model, AWS is responsible for "Security of the Cloud". This includes 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.

Replacing faulty hardware of Amazon EC2 instances - Replacing faulty hardware of Amazon EC2 instances comes under the infrastructure maintenance "of" the cloud. This is the responsibility of AWS.

Operating the infrastructure layer, the operating system and the platform for the Amazon S3 service - 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.

Shared Responsibility Model Overview:



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

Incorrect options:

Enabling Multi Factor Authentication on AWS accounts in your organization - Enabling Multi Factor Authentication for AWS accounts in your organization is your responsibility. On the other hand, AWS is responsible for making sure that the user data created and their relationships and policies are stored on fail-proof infrastructure.

Creating IAM role for accessing Amazon EC2 instances - Creating user roles, policies is the responsibility of the customer. Customers will decide "which" resources get "what" access.

Creating S3 bucket policies for appropriate user access - Creating bucket policies for Amazon S3 data access is the responsibility of the customer. The customer decides who gets access to the data he stores on S3 and will use AWS tools to implement these requirements. AWS on the other hand is responsible for keeping the data safe from hardware and software failure.

Reference:

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

Domain
Security and Compliance

Question 10
Which option is a common stakeholder role for the AWS Cloud Adoption Framework (AWS CAF) platform perspective? (Select two)

1] Chief Information Officer (CIO)
2] Chief Data Officer (CDO)
3] Chief Product Officer (CPO)
4] Chief Technology Officer (CTO)
5] Engineer

Overall explanation
Correct option:

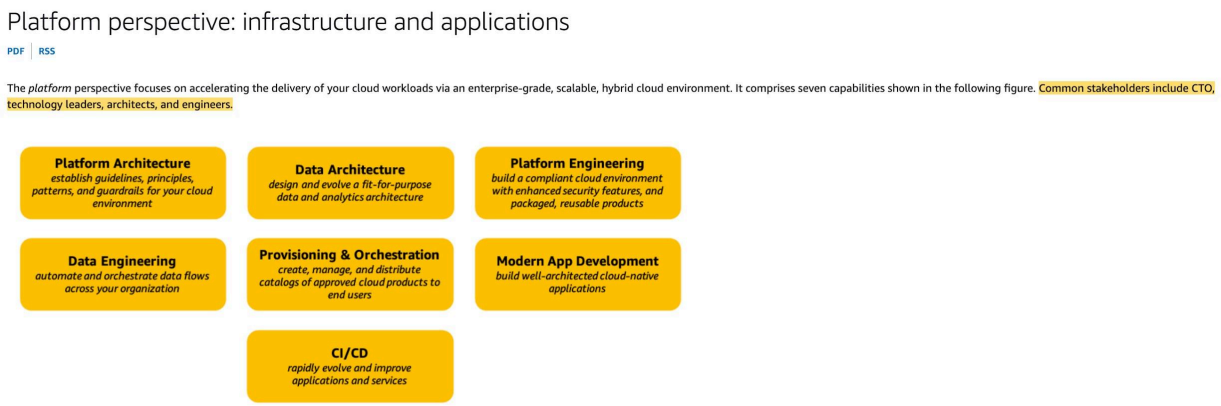
Engineer

Chief Technology Officer (CTO)

The AWS Cloud Adoption Framework (AWS CAF) leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations. These capabilities provide best practice guidance that helps you improve your cloud readiness. AWS CAF groups its capabilities in six perspectives: Business, People, Governance, Platform, Security, and Operations.

The platform perspective focuses on accelerating the delivery of your cloud workloads via an enterprise-grade, scalable, hybrid cloud environment. It comprises seven capabilities shown in the following figure. Common stakeholders include Chief Technology Officer (CTO), technology leaders, architects, and engineers.

The AWS Cloud Adoption Framework (AWS CAF) platform perspective:



via - https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/platform-perspective.html

Incorrect options:

Chief Product Officer (CPO)

Chief Data Officer (CDO)

Chief Information Officer (CIO)

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

References:

https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/platform-perspective.html

https://d1.awsstatic.com/whitepapers/aws-caf-ebook.pdf

Domain
Cloud Concepts

Question 11
Which of the following AWS services support reservations to optimize costs? (Select three)

1] Amazon DocumentDB
2] Amazon Simple Storage Service (Amazon S3)
3] Amazon Relational Database Service (Amazon RDS)
4] Amazon Elastic Compute Cloud (Amazon EC2)
5] AWS Lambda
6] Amazon DynamoDB

Overall explanation
Correct options:

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon DynamoDB

Amazon Relational Database Service (Amazon RDS)

The following AWS services support reservations to optimize costs:

Amazon EC2 Reserved Instances (RI): You can use Amazon EC2 Reserved Instances (RI) to reserve capacity and receive a discount on your instance usage compared to running On-Demand instances.

Amazon DynamoDB Reserved Capacity: If you can predict your need for Amazon DynamoDB read-and-write throughput, Reserved Capacity offers significant savings over the normal price of DynamoDB provisioned throughput capacity.

Amazon ElastiCache Reserved Nodes: Amazon ElastiCache Reserved Nodes give you the option to make a low, one-time payment for each cache node you want to reserve and, in turn, receive a significant discount on the hourly charge for that node.

Amazon RDS RIs: Like Amazon EC2 RIs, Amazon RDS RIs can be purchased using No Upfront, Partial Upfront, or All Upfront terms. All Reserved Instance types are available for Aurora, MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines.

Amazon Redshift Reserved Nodes: If you intend to keep an Amazon Redshift cluster running continuously for a prolonged period, you should consider purchasing reserved-node offerings. These offerings provide significant savings over on-demand

pricing, but they require you to reserve compute nodes and commit to paying for those nodes for either a 1- or 3-year duration.

Incorrect options:

Amazon DocumentDB - Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. As a document database, Amazon DocumentDB makes it easy to store, query, and index JSON data.

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

None of these AWS services support reservations to optimize costs.

Reference:

https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf

Domain
Billing and Pricing

Question 12
Which of the following is an AWS database service?
1] AWS Database Migration Service (AWS DMS)
2] Amazon Redshift
3] AWS Storage Gateway
4] AWS Glue

Overall explanation
Correct option:

Amazon Redshift

Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for large scale data set storage and analysis.

Incorrect options:

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

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that connects your existing on-premises environments with the AWS Cloud. Customers use AWS Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases.

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

References:

https://aws.amazon.com/redshift/

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

Domain
Technology

Question 13
A unicorn startup is building an analytics application with support for a speech-based interface. The application will accept speech-based input from users and then convey results via speech. As a Cloud Practitioner, which solution would you recommend for the given use-case?

1] Use Amazon Transcribe to convert speech to text for downstream analysis. Then use Amazon Polly to convey the text results via speech

2] Use Amazon Polly to convert speech to text for downstream analysis. Then use Amazon Transcribe to convey the text results via speech

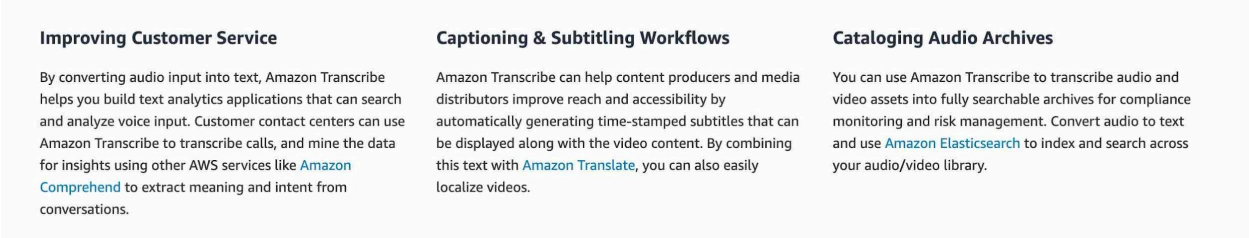
3] Use Amazon Polly to convert speech to text for downstream analysis. Then use Amazon Translate to convey the text results via speech
4] Use Amazon Translate to convert speech to text for downstream analysis. Then use Amazon Polly to convey the text results via speech

Overall explanation
Correct option:

Use Amazon Transcribe to convert speech to text for downstream analysis. Then use Amazon Polly to convey the text results via speech

You can use Amazon Transcribe to add speech-to-text capability to your applications. Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly and accurately. Amazon Transcribe can be used to transcribe customer service calls, to automate closed captioning and subtitling, and to generate metadata for media assets.

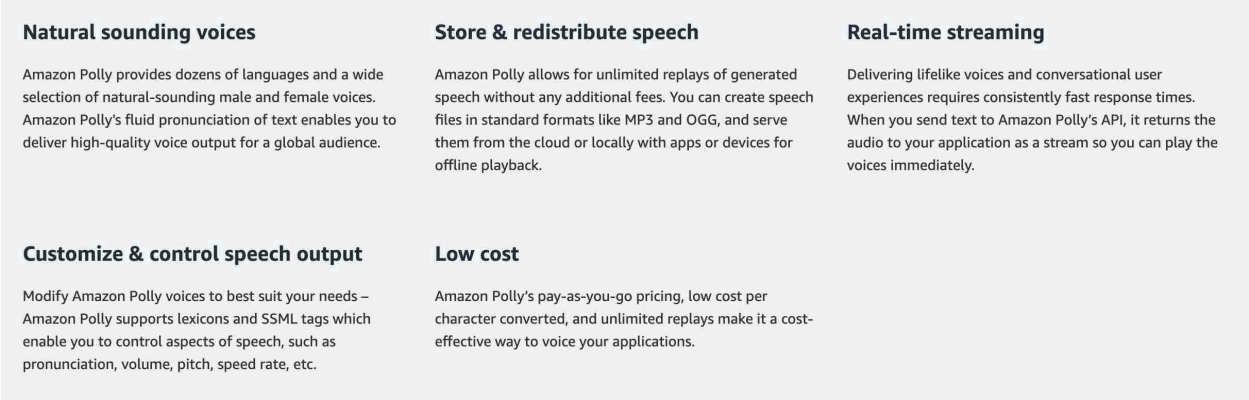
Amazon Transcribe Use-Cases:



via - https://aws.amazon.com/transcribe/

You can use Amazon Polly to turn text into lifelike speech thereby allowing you to create applications that talk. Polly's Text-to-Speech (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech.

Amazon Polly Benefits:



via - https://aws.amazon.com/polly/

Amazon Translate is used for language translation. Amazon Translate uses neural machine translation via deep learning models to deliver more accurate and more natural-sounding translation than traditional statistical and rule-based translation algorithms.

Incorrect options:

Use Amazon Polly to convert speech to text for downstream analysis. Then use Amazon Transcribe to convey the text results via speech - Amazon Polly cannot be used to convert speech to text, so this option is incorrect.

Use Amazon Translate to convert speech to text for downstream analysis. Then use Amazon Polly to convey the text results via speech - Amazon Translate cannot convert speech to text, so this option is incorrect.

Use Amazon Polly to convert speech to text for downstream analysis. Then use Amazon Translate to convey the text results via speech - Amazon Polly cannot be used to convert speech to text, so this option is incorrect.

References:

https://aws.amazon.com/transcribe/

https://aws.amazon.com/polly/

Domain
Technology

Question 14

A financial services company wants to ensure that its AWS account activity meets the governance, compliance and auditing norms. As a Cloud Practitioner, which AWS service would you recommend for this use-case?

1] Amazon CloudWatch

2] AWS CloudTrail

3] AWS Trusted Advisor

4] AWS Config

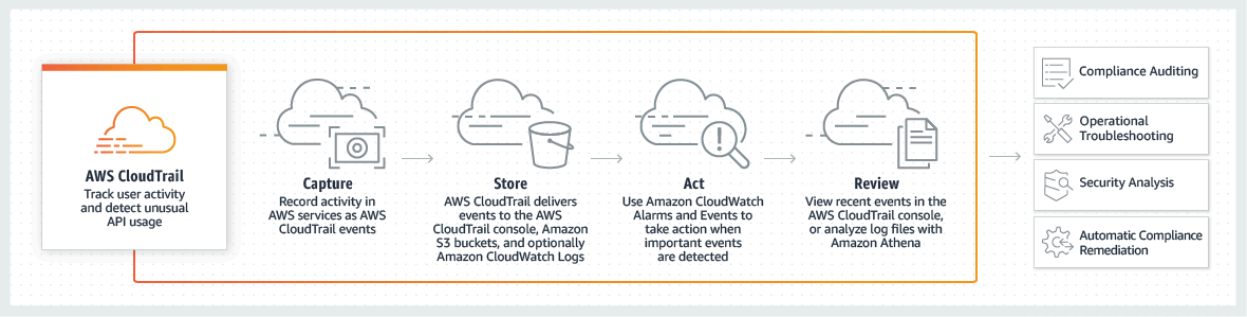
Overall explanation

Correct option:

AWS CloudTrail

You can use CloudTrail to log, monitor and retain account activity related to actions across your AWS infrastructure. CloudTrail provides an event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services.

How CloudTrail Works:



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

Incorrect options:

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.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems.

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 on cost optimization, security, fault tolerance, service limits and performance improvement.

Exam Alert:

You may see use-cases asking you to select one of CloudWatch vs CloudTrail vs Config. Just remember this thumb rule -

Think resource performance monitoring, events, and alerts; think CloudWatch.

Think account-specific activity and audit; think CloudTrail.

Think resource-specific change history, audit, and compliance; think Config.

Reference:

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

Domain
Cloud Concepts

Question 15
An IT company is planning to migrate from an on-premises environment to AWS Cloud. Which of the following expense areas would result in cost savings when the company moves to AWS Cloud? (Select two)

1] Project manager salary
2] Data center physical security expenditure
3] Data center hardware infrastructure expenditure
4] Developer salary
5] SaaS application license fee

Overall explanation
Correct options:

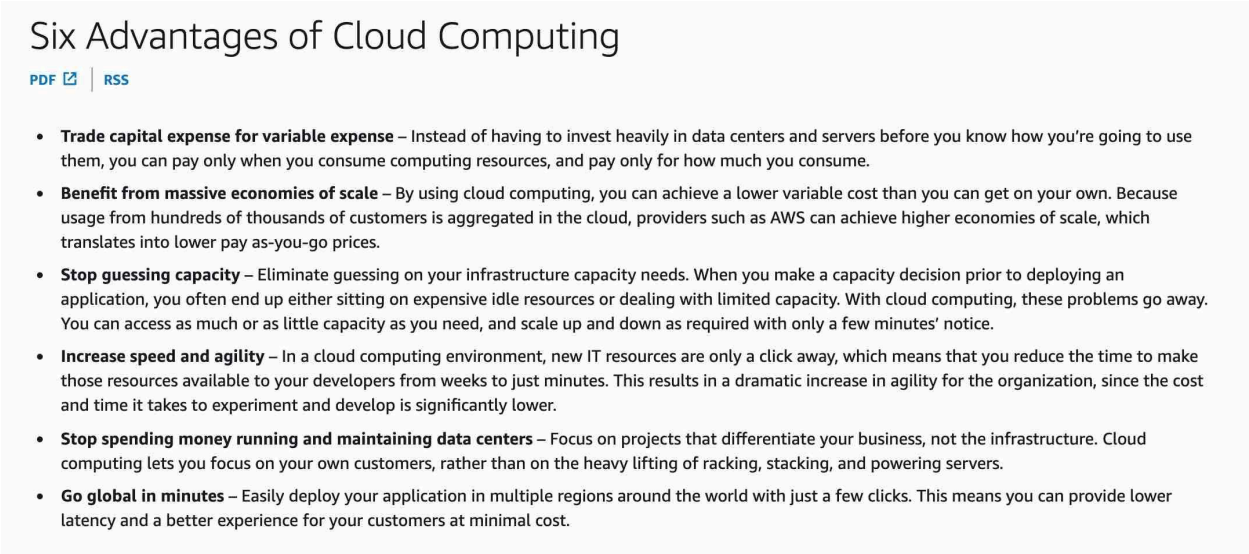
Data center hardware infrastructure expenditure

Data center physical security expenditure

The company does not need to spend on the computing hardware infrastructure and data center physical security. So these expense areas would result in cost savings. The expenditure on the SaaS application license fee, developer salary, and project manager salary would remain the same.

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:



Six Advantages of Cloud Computing

PDF | RSS

- **Trade capital expense for variable expense** – 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.
- **Benefit from massive economies of scale** – 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.
- **Stop guessing capacity** – Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often end up either sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. 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.
- **Increase speed and agility** – 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.
- **Stop spending money running and maintaining data centers** – Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers.
- **Go global in minutes** – 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.

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

Incorrect options:

SaaS application license fee

Developer salary

Project manager salary

As explained earlier, the expenditure on the SaaS application license fee, developer salary, and project manager salary would remain the same, so these options are incorrect.

Reference:

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

Domain
Cloud Concepts

Question 16
Which of the following is an INCORRECT statement about Scaling, a design principle of Reliability pillar of the AWS Well-Architected Framework?

1] Fault tolerance is achieved by a scale up operation
2] Fault tolerance is achieved by a scale out operation
3] A scale out operation implies you scale by adding more instances to your existing pool of resources
4] A scale up operation implies you scale by adding more power (CPU, RAM) to your existing machine/node

Overall explanation
Correct option: **Fault tolerance is achieved by a scale up operation**

A scale up operation is constrained to be 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 CPUs, memory or storage. Fault tolerance is not possible for such scaling operations since a single instance is prone to failure.

Incorrect options:

A scale up operation implies you scale by adding more power (CPU, RAM) to your existing machine/node - A scale up operation runs on a single instance. Adding power is only possible through the addition of resources in the form of CPU, RAM, or storage to enhance performance.

A scale out operation implies you scale by adding more instances to your existing pool of resources - A scale out operation is one that can increase capacity by adding more computers to the system. Scale out systems are oftentimes able to outperform scale up systems by enabling parallel execution of workloads and distributing those across many different computers.

Fault tolerance is achieved by a scale out operation - A scale out operation adds more instances to an existing pool of instances. This implies, there is no single point of failure. If an instance is down, the workload is taken up by other healthy instances. Distributed systems are an example of such scaling.

Reference:

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

Domain
Cloud Concepts

Question 17
A multi-national company has just moved its infrastructure from its on-premises data center to AWS Cloud. As part of the shared responsibility model, AWS is responsible for which of the following?

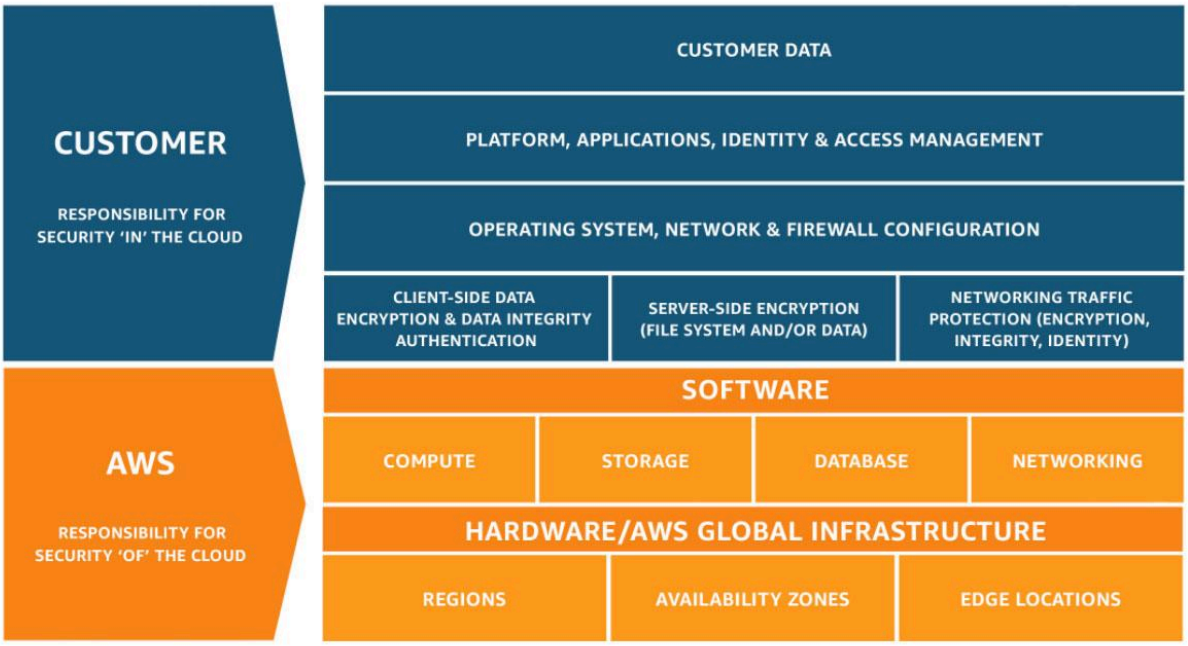
1] Patching guest OS
2] Service and Communications Protection or Zone Security
3] Configuring customer applications
4] Physical and Environmental controls

Overall explanation
Correct option:

Physical and Environmental controls

As part of the shared responsibility model, Physical and Environmental controls are part of the inherited controls and hence these are the responsibility of AWS.

Shared Responsibility Model Overview:



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

Incorrect options:

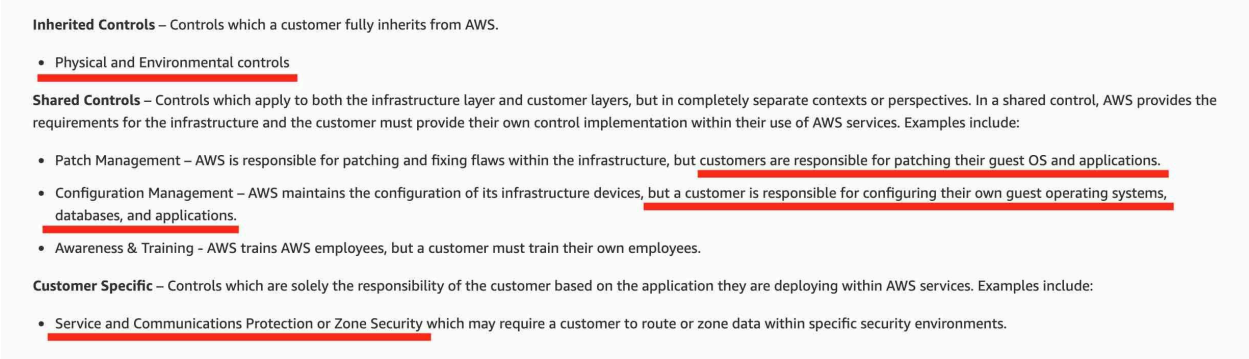
Patching guest OS

Configuring customer applications

The customers must provide their own control implementation within their use of AWS services. Therefore, the customers are responsible for patching their guest OS as well as for configuring their applications.

Service and Communications Protection or Zone Security - Customers are responsible for Service and Communications Protection or Zone Security which may require the customers to route or zone data within specific security environments.

Please review the IT controls under the Shared Responsibility Model:



Inherited Controls – Controls which a customer fully inherits from AWS.

- Physical and Environmental controls

Shared Controls – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

Customer Specific – Controls which are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:

- Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

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

Reference:

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

Domain
Cloud Concepts

Question 18
A startup wants to provision an EC2 instance for the lowest possible cost for a long-term duration but needs to make sure that the instance would never be interrupted. As a Cloud Practitioner, which of the following options would you recommend?

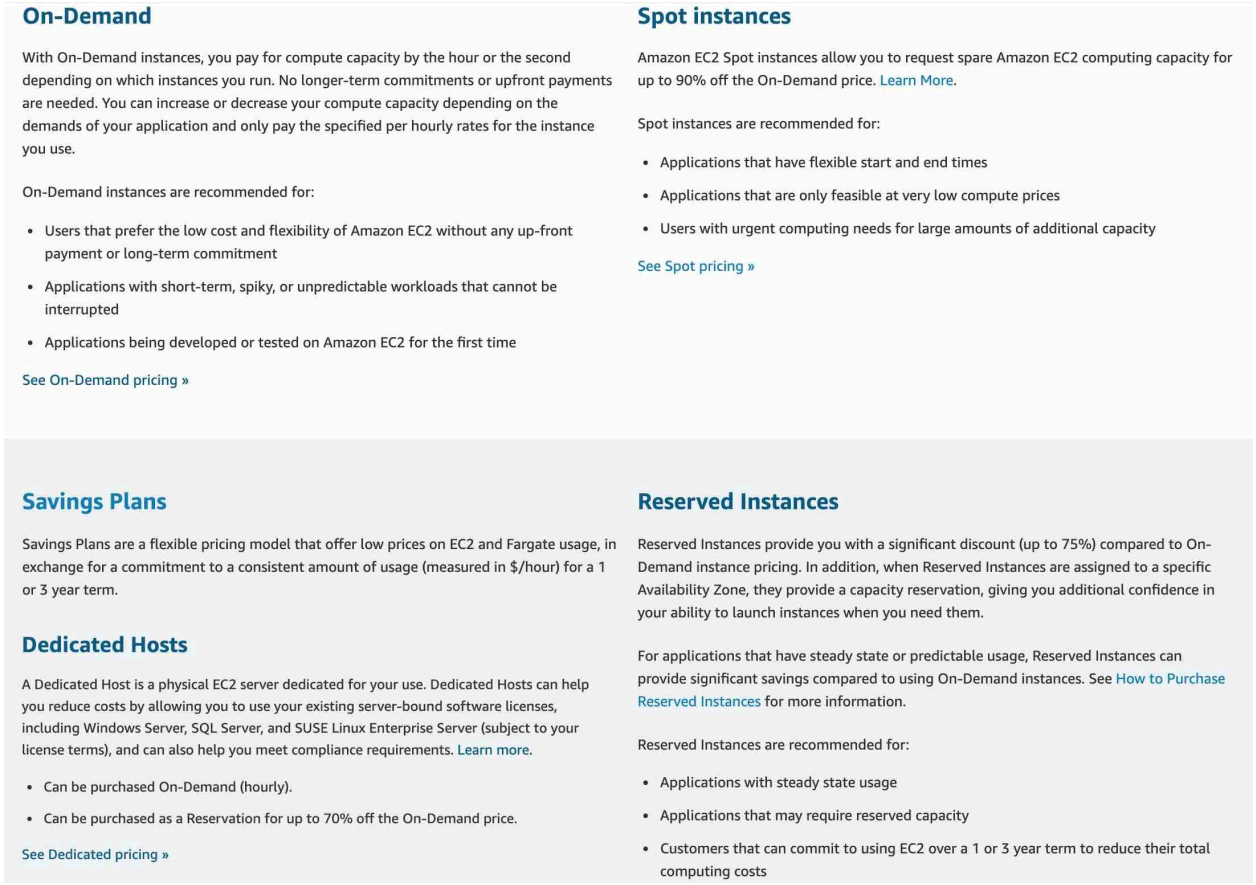
1] EC2 Dedicated Host
2] EC2 Spot Instance
3] EC2 On-Demand Instance
4] EC2 Reserved Instance (RI)

Overall explanation
Correct option:

EC2 Reserved Instance (RI)

An EC2 Reserved Instance (RI) provides you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. A Reserved Instance (RI) is not a physical instance, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance (RI) for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. A reserved instance (RI) cannot be interrupted. So this is the correct option.

EC2 Pricing Options Overview:



via - https://aws.amazon.com/ec2/pricing/

Incorrect options:

EC2 On-Demand Instance - An EC2 On-Demand Instance is an instance that you use on-demand. You have full control over its lifecycle — you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you pay only for the seconds that your On-Demand Instances are running. The price per second for running an On-Demand Instance is fixed. On-demand instances cannot be interrupted. However, On-demand instances are not as cost-effective as Reserved instances, so this option is not correct.

EC2 Spot Instance - An EC2 Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts (up to 90%), you can lower your Amazon EC2

costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time. So this option is not correct for the given use-case.

EC2 Dedicated Host - An Amazon EC2 Dedicated Host allows 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 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 requirement. It is not cost-efficient compared to an On-Demand instance. So this option is not correct.

Reference:

https://aws.amazon.com/ec2/pricing/

Domain
Billing and Pricing

Question 19
Which of the following statements are CORRECT regarding the AWS VPC service? (Select two)

1] A Network Address Translation instance (NAT instance) is managed by AWS
2] A Security Group can have allow rules only
3] A network access control list (network ACL) can have allow rules only
4] A Network Address Translation gateway (NAT gateway) is managed by AWS
5] A Security Group can have both allow and deny rules

Overall explanation
Correct options:

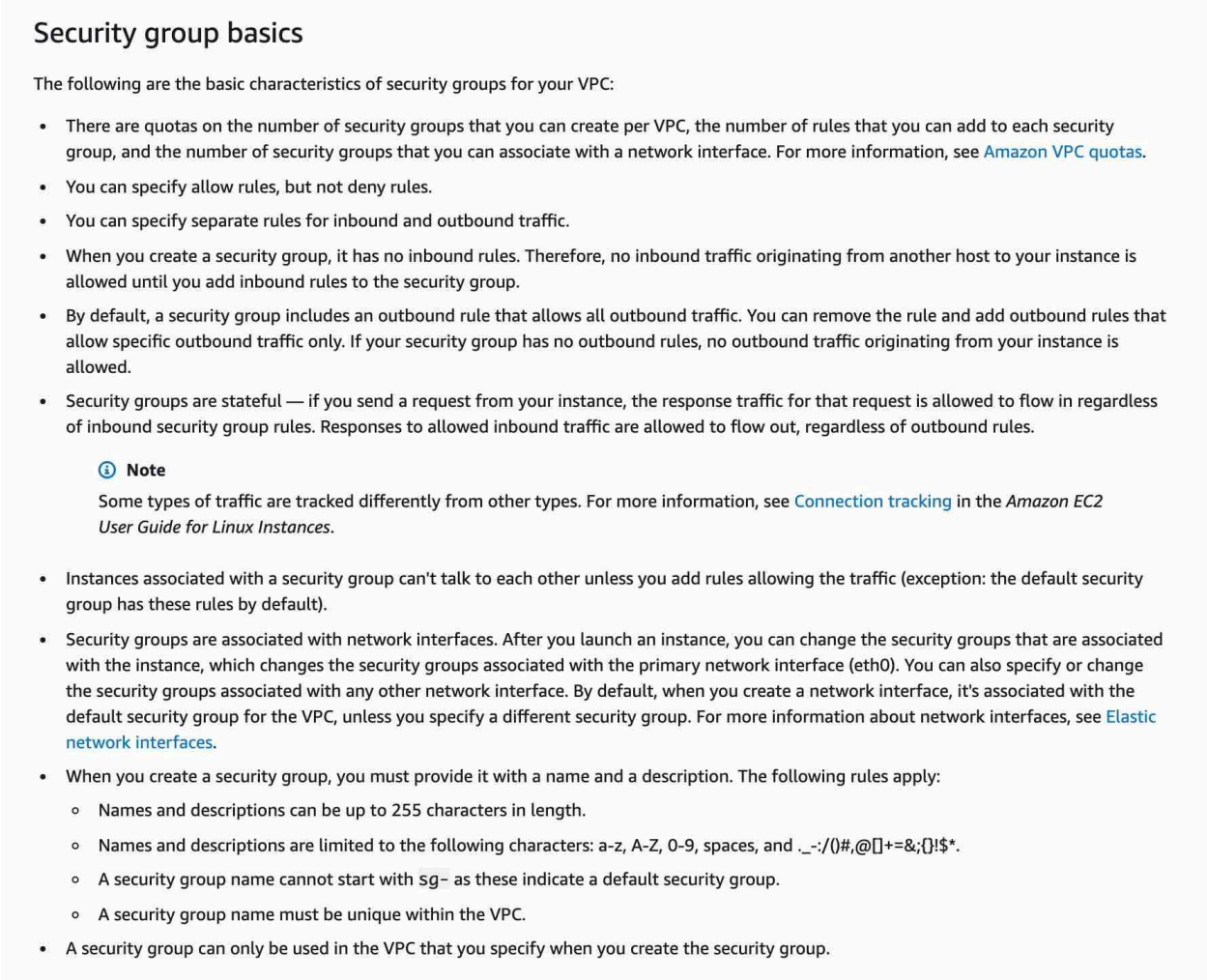
A Security Group can have allow rules only

A Network Address Translation gateway (NAT gateway) is managed by AWS

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.

Security Group Overview:



Security group basics

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

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

  Note

  Some types of traffic are tracked differently from other types. For more information, see Connection tracking in the *Amazon EC2 User Guide for Linux Instances*.

- Instances associated with a security group can't talk to each other unless you add rules allowing the traffic (exception: the default security group has these rules by default).
- Security groups are associated with network interfaces. After you launch an instance, you can change the security groups that are associated with the instance, which changes the security groups associated with the primary network interface (eth0). You can also specify or change the security groups associated with any other network interface. By default, when you create a network interface, it's associated with the default security group for the VPC, unless you specify a different security group. For more information about network interfaces, see Elastic network interfaces.
- When you create a security group, you must provide it with a name and a description. The following rules apply:
  - Names and descriptions can be up to 255 characters in length.
  - Names and descriptions are limited to the following characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*.
  - A security group name cannot start with `sg-` as these indicate a default security group.
  - A security group name must be unique within the VPC.
- A security group can only be used in the VPC that you specify when you create the security group.

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

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 (i.e. it works at 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:

Network ACL basics

The following are the basic things that you need to know about network ACLs:

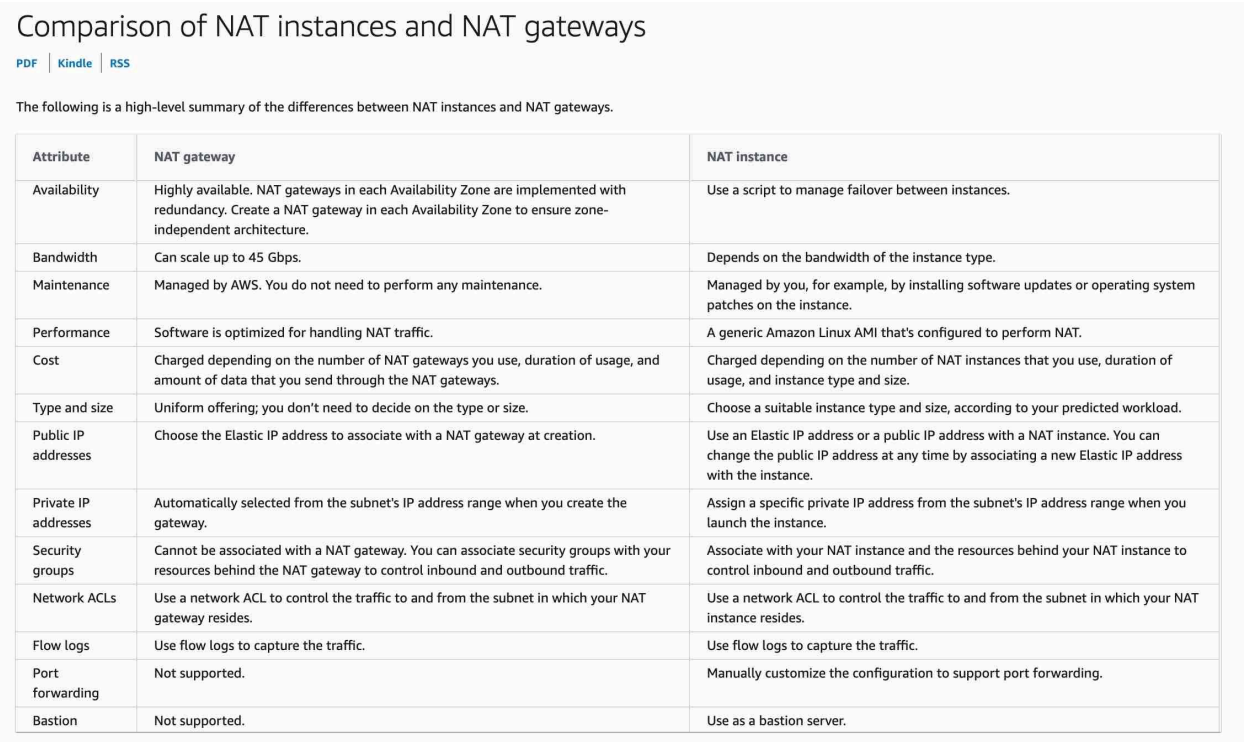
- Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.
- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
- You can associate a network ACL with multiple subnets. However, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- A network ACL contains a numbered list of rules. We evaluate the rules in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. We recommend that you start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules where you need to later on.
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

There are quotas (limits) for the number of network ACLs per VPC, and the number of rules per network ACL. For more information, see Amazon VPC quotas.

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

You can use a network address translation (NAT) gateway or a Network Address Translation instance (NAT instance) to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. Network Address Translation gateway (NAT gateway) is managed by AWS but Network Address Translation instance (NAT instance) is managed by you.

Please see this comparison table for differences between Network Address Translation gateway (NAT gateway) and Network Address Translation instance (NAT instance):



Comparison of NAT instances and NAT gateways

PDF | Kindle | RSS

The following is a high-level summary of the differences between NAT instances and NAT gateways.

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Can scale up to 45 Gbps.	Depends on the bandwidth of the instance type.
Maintenance	Managed by AWS. You do not need to perform any maintenance.	Managed by you, for example, by installing software updates or operating system patches on the instance.
Performance	Software is optimized for handling NAT traffic.	A generic Amazon Linux AMI that's configured to perform NAT.
Cost	Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.	Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size.
Type and size	Uniform offering; you don't need to decide on the type or size.	Choose a suitable instance type and size, according to your predicted workload.
Public IP addresses	Choose the Elastic IP address to associate with a NAT gateway at creation.	Use an Elastic IP address or a public IP address with a NAT instance. You can change the public IP address at any time by associating a new Elastic IP address with the instance.
Private IP addresses	Automatically selected from the subnet's IP address range when you create the gateway.	Assign a specific private IP address from the subnet's IP address range when you launch the instance.
Security groups	Cannot be associated with a NAT gateway. You can associate security groups with your resources behind the NAT gateway to control inbound and outbound traffic.	Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic.
Network ACLs	Use a network ACL to control the traffic to and from the subnet in which your NAT gateway resides.	Use a network ACL to control the traffic to and from the subnet in which your NAT instance resides.
Flow logs	Use flow logs to capture the traffic.	Use flow logs to capture the traffic.
Port forwarding	Not supported.	Manually customize the configuration to support port forwarding.
Bastion	Not supported.	Use as a bastion server.

via - https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

Incorrect options:

A Security Group can have both allow and deny rules

A Network Address Translation instance (NAT instance) is managed by AWS

A network access control list (network ACL) can have allow rules only

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

References:

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

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

Domain

Cloud Concepts

Question 20
Which of the following AWS Support plans provide access to only core checks from the AWS Trusted Advisor Best Practice Checks? (Select two)

1] AWS Business Support

2] AWS Basic Support

3] AWS Enterprise Support

4] AWS Developer Support

5] AWS Enterprise On-Ramp Support

Overall explanation
Correct options:

AWS Basic Support

The AWS Basic Support plan only provides access to the following:

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Health - Your Account Health Dashboard : A personalized view of the health of your AWS services, and alerts when your resources are impacted.

AWS Developer Support

You should use the AWS Developer Support plan if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours as well as general architectural guidance as you build and test. This plan provides access to just the core Trusted Advisor checks from the Service Quota and basic Security checks.

Exam Alert:

Please review the differences between the AWS Developer Support, AWS Business Support, AWS Enterprise On-Ramp Support and AWS Enterprise Support plans as you can expect at least a couple of questions on the exam:

	Developer	Business	Enterprise On-Ramp	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Minimum recommended tier if you have production workloads in AWS*	*Recommended if you have production and/or business critical workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
AWS Trusted Advisor Best Practice Checks	Service Quota and basic Security checks	Full set of checks	Full set of checks	Full set of checks
AWS Trusted Advisor Priority				Prioritized recommendations curated by your AWS account team
Enhanced Technical Support	Business hours** web access to Cloud Support Associates Unlimited cases with 1 primary contact Prioritized responses on AWS re:Post	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack
Case Severity / Response Times*	General guidance: < 24 hours** System impaired: < 12 hours**	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 30 minutes	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business/Mission-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications (one-per-year)	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API	AWS Support API

	Developer *Recommended if you are experimenting or testing in AWS.*	Business *Minimum recommended tier if you have production workloads in AWS*	Enterprise On-Ramp *Recommended if you have production and/or business critical workloads in AWS.*	Enterprise *Recommended if you have business and/or mission critical workloads in AWS.*
Third-Party Software Support		Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting
Proactive Programs and Self Service	Access to Support Automation Workflows with prefixes AWSSupport	Access to Infrastructure Event Management for additional fee Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport	Infrastructure Event Management (one-per-year) Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport	Infrastructure Event Management Access to proactive reviews, workshops, and deep dives Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport
AWS Incident Detection and Response				Access to AWS Incident Detection and Response **for an additional fee**. AWS Incident Detection and Response is an add-on to Enterprise Support that offers 24x7 proactive monitoring and incident management for selected workloads. AWS Incident Detection and Response leverages the proven operational, enhanced monitoring, and incident management capabilities used internally by AWS teams and externally by AWS Managed Services (AMS).
AWS Managed Services		Access to AWS Managed Services (AMS) **for an additional fee**. AMS augments your existing teams with cloud advanced operations skills and capacity. Includes baseline operations, a designated Cloud Service Delivery Manager (CSDM), Cloud Architect (CA), and access to the AMS security team.	Access to AWS Managed Services (AMS) **for an additional fee**. AMS augments your existing teams with cloud advanced operations skills and capacity. Includes baseline operations, a designated Cloud Service Delivery Manager (CSDM), Cloud Architect (CA), and access to the AMS security team.	Access to AWS Managed Services (AMS) **for an additional fee**. AMS augments your existing teams with cloud operations skills and capacity. It includes baseline operations, a designated Cloud Service Delivery Manager (CSDM), Cloud Architect (CA), and access to the AMS security team. AWS Incident Detection and Response is available at no additional charge in eligible regions for AWS Managed Services direct customers with AWS Enterprise Support.

	Developer *Recommended if you are experimenting or testing in AWS.*	Business *Minimum recommended tier if you have production workloads in AWS*	Enterprise On-Ramp *Recommended if you have production and/or business critical workloads in AWS.*	Enterprise *Recommended if you have business and/or mission critical workloads in AWS.*
Technical Account Management			A pool of Technical Account Managers to provide proactive guidance, and coordinate access to programs and AWS experts	Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization and coordinate access to programs and AWS experts
Training				Access to online self-paced labs
Account Assistance			Concierge Support Team	Concierge Support Team
Pricing *Additional services for **additional fee**	Greater of $29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of $100 / month*** - or - 10% of monthly AWS usage for the first $0–$10K 7% of monthly AWS usage from $10K–$80K 5% of monthly AWS usage from $80K–$250K 3% of monthly AWS usage over $250K See pricing detail and example. *Access to AWS Managed Services (AMS) **for an additional fee**	Greater of $5,500 - or - 10% of monthly AWS usage See pricing detail and example. *Access to AWS Managed Services (AMS) **for an additional fee**	Greater of $15,000 - or - 10% of monthly AWS usage for the first $0–$150K 7% of monthly AWS usage from $150K–$500K 5% of monthly AWS usage from $500K–$1M 3% of monthly AWS usage over $1M See pricing detail and example. * Access to AWS Incident Detection and Response **for an additional fee.** *Access to AWS Managed Services (AMS) **for an additional fee**

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

Incorrect options:

AWS Enterprise Support - AWS Enterprise Support plan provides customers with concierge-like service where the main focus is helping the customer achieve their outcomes and find success in the cloud. With AWS Enterprise Support, you get 24x7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative architectural guidance and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts. You also get full access to AWS Trusted Advisor Best Practice Checks.

AWS Business Support - You should use the AWS Business Support plan if you have production workloads on AWS and want 24x7 phone, email and chat access to technical

support and architectural guidance in the context of your specific use-cases. You also get full access to AWS Trusted Advisor Best Practice Checks.

AWS Enterprise On-Ramp Support - You should use the AWS Enterprise On-Ramp Support plan if you have production/business critical workloads in AWS and want 24x7 access to technical support and need expert guidance to grow and optimize in the Cloud. You get full access to AWS Trusted Advisor Best Practice Checks.

Reference:

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

Domain
Cloud Concepts

Question 21
A big data analytics company is moving its IT infrastructure from an on-premises data center to AWS Cloud. The company has some server-bound software licenses that it wants to use on AWS. As a Cloud Practitioner, which of the following EC2 instance types would you recommend to the company?

1] Dedicated Instance
2] Dedicated Host
3] Reserved Instance (RI)
4] On-Demand Instance

Overall explanation
Correct option:

Dedicated Host

Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirements.

Exam Alert:

Please review the differences between Dedicated hosts and Dedicated instances:

Differences between Dedicated Hosts and Dedicated Instances

Dedicated Hosts and Dedicated Instances can both be used to launch Amazon EC2 instances onto physical servers that are dedicated for your use.

There are no performance, security, or physical differences between Dedicated Instances and instances on Dedicated Hosts. However, there are some differences between the two. The following table highlights some of the key differences between Dedicated Hosts and Dedicated Instances:

	Dedicated Host	Dedicated Instance
Billing	Per-host billing	Per-instance billing
Visibility of sockets, cores, and host ID	Provides visibility of the number of sockets and physical cores	No visibility
Host and instance affinity	Allows you to consistently deploy your instances to the same physical server over time	Not supported
Targeted instance placement	Provides additional visibility and control over how instances are placed on a physical server	Not supported
Automatic instance recovery	Supported. For more information, see Host recovery.	Supported
Bring Your Own License (BYOL)	Supported	Not supported

via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-hosts-overview.html

Incorrect options:

Dedicated Instance - A Dedicated Instance is an Amazon EC2 instance that runs in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at the hardware

level. However, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances. You cannot use Dedicated Instances for using server-bound software licenses.

Reserved Instance (RI) - A Reserved Instance (RI) provides you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. A Reserved Instance (RI) is not a physical instance, but rather a billing discount applied to the use of an On-Demand Instance in your account. You can purchase a Reserved Instance (RI) for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. You cannot use a Reserved Instance (RI) for using server-bound software licenses.

On-Demand Instance - An On-Demand Instance is an instance that you use on-demand. You have full control over its lifecycle — you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you pay only for the seconds that your On-Demand Instances are running. The price per second for running an On-Demand Instance is fixed. On-demand instances cannot be interrupted. You cannot use On-demand Instances for using server-bound software licenses.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-hosts-overview.html

Domain
Technology

Question 22
Which AWS Service can be used to mitigate a Distributed Denial of Service (DDoS) attack?

1] AWS Shield
2] AWS Key Management Service (AWS KMS)
3] Amazon CloudWatch
4] AWS Systems Manager
5] Overall explanation

Correct option:

AWS Shield

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

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall.

Incorrect options:

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems.

AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources.

AWS Key Management Service (AWS KMS) - AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys.

Reference:

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

Domain
Security and Compliance

Question 23
Which of the following is a recommended way to provide programmatic access to AWS resources?

1] Use AWS Multi-Factor Authentication (AWS MFA) to access AWS resources programmatically
2] Create a new IAM user and share the username and password
3] Use IAM user group to access AWS resources programmatically
4] Use Access Key ID and Secret Access Key to access AWS resources programmatically

Overall explanation
Correct option:

Use Access Key ID and Secret Access Key to access AWS resources programmatically

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 and a secret access key. As a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. When you create an access key pair, save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must delete the access key and create a new one.

Incorrect options:

Create a new IAM user and share the username and password - This is not a viable option, IAM user credentials are not needed to access resources programmatically.

Use AWS Multi-Factor Authentication (AWS MFA) to access AWS resources programmatically - For increased security, AWS recommends that you configure AWS Multi-Factor Authentication (AWS MFA) to help protect your AWS resources. You can enable MFA for IAM users or the AWS account root user. MFA adds extra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services. MFA cannot be used for programmatic access to AWS resources.

Use IAM user group to access AWS resources programmatically - An IAM user group is a collection of IAM users. An IAM user group lets you specify permissions for multiple users, which can make it easier to manage the permissions for those users. IAM user group is for managing users and not for programmatic access to AWS resources.

Reference:

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

Domain
Security and Compliance

Question 24
An e-commerce company has deployed an RDS database in a single Availability Zone (AZ). The engineering team wants to ensure that in case of an AZ outage, the database should continue working on the same endpoint without any manual administrative intervention. Which of the following solutions can address this use-case?

1] Provision the database via AWS CloudFormation

2] Deploy the database via AWS Elastic Beanstalk

3] Configure the database in RDS Multi-AZ deployment with automatic failover to the standby

4] Configure the database in RDS read replica mode with automatic failover to the standby

Overall explanation
Correct option:

Configure the database in RDS Multi-AZ deployment with automatic failover to the standby

When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

Incorrect options:

Deploy the database via AWS Elastic Beanstalk - You cannot deploy only a database via Elastic Beanstalk as its meant for automatic application deployment when you upload your code. Then Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Hence this option is incorrect.

Configure the database in RDS read replica mode with automatic failover to the standby - For RDS, Read replicas allow you to create read-only copies that are synchronized with your master database. There is no standby available while using read replicas. In case of infrastructure failure, you have to manually promote the read replica to be its own standalone DB Instance, which means that the database endpoint would change. Therefore, this option is incorrect.

Provision the database via AWS CloudFormation - You can provision the database via CloudFormation for sure, however, it does not provide any automatic recovery in case of a disaster.

References:

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

Domain
Cloud Concepts

Question 25
A company needs a storage solution for a project wherein the data is accessed less frequently but needs rapid access when required. Which S3 storage class is the MOST cost-effective for the given use-case?
1] Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
2] Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)
3] Amazon S3 Standard
4] Amazon S3 Glacier (S3 Glacier)

Overall explanation
Correct option:

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 make

S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files.

Incorrect options:

Amazon S3 Standard - The Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. S3 standard would turn out to be costlier than S3 Standard-IA for the given use-case, so this option is not correct.

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) - The Amazon S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. S3 Intelligent-Tiering would turn out to be costlier than S3 Standard-IA for the given use-case, so this option is not correct.

Amazon S3 Glacier (S3 Glacier) - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. S3 Glacier does not support rapid data retrieval, so this option is ruled out.

Reference:

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

Domain
Technology

Question 26
A cyber forensics team has detected that AWS owned IP-addresses are being used to carry out malicious attacks. As this constitutes prohibited use of AWS services, which of the following is the correct solution to address this issue?

1] Contact AWS Developer Forum moderators

2] Contact AWS Abuse Team

3] Contact AWS Support
4] Write an email to Jeff Bezos, the founder of Amazon, with the details of the incident

Overall explanation
Correct option:

Contact AWS Abuse Team

The AWS Abuse team can assist you when AWS resources are used to engage in abusive behavior.

Please see details of the various scenarios that the AWS Abuse team can address:

How do I report abuse of AWS resources?

Last updated: 2020-04-30

I suspect that Amazon Web Services (AWS) resources are used for abusive or illegal purposes. How do I let AWS know?

Resolution

The AWS Abuse team can assist you when AWS resources are used to engage in the following types of abusive behavior:

- **Spam:** You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are used to spam websites or forums.
- **Port scanning:** Your logs show that one or more AWS-owned IP addresses are sending packets to multiple ports on your server, and you believe this is an attempt to discover unsecured ports.
- **Denial-of-service (DoS) attacks:** Your logs show that one or more AWS-owned IP addresses are used to flood ports on your resources with packets, and you believe that this is an attempt to overwhelm or crash your server or the software running on your server.
- **Intrusion attempts:** Your logs show that one or more AWS-owned IP addresses are used to attempt to log in to your resources.
- **Hosting objectionable or copyrighted content:** You have evidence that AWS resources are used to host or distribute illegal content or distribute copyrighted content without the consent of the copyright holder.
- **Distributing malware:** You have evidence that AWS resources are used to distribute software that was knowingly created to compromise or cause harm to computers or machines on which it is installed.

via - https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/

Incorrect options:

Contact AWS Support - You need to contact the AWS Abuse team for prohibited use of AWS services.

Contact AWS Developer Forum moderators - You need to contact the AWS Abuse team for prohibited use of AWS services.

Write an email to Jeff Bezos, the founder of Amazon, with the details of the incident - This has been added as a distractor. For the record, please let us know if you do get a reply from Mr. Bezos.

Reference:

https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/

Domain
Security and Compliance

Question 27
A silicon valley based healthcare startup stores anonymized patient health data on Amazon S3. The CTO further wants to ensure that any sensitive data on S3 is discovered and identified to prevent any sensitive data leaks. As a Cloud Practitioner, which AWS service would you recommend addressing this use-case?

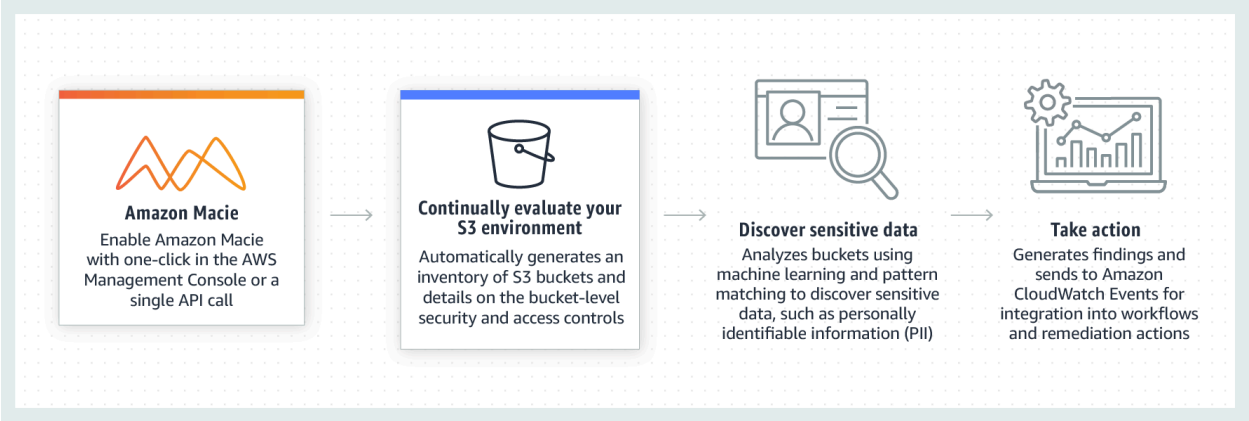
1] AWS Glue
2] Amazon Polly
3] AWS Secrets Manager
4] Amazon Macie

Overall explanation
Correct option:

Amazon Macie

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).

How Macie Works:



via - https://aws.amazon.com/macie/

Incorrect options:

AWS Glue - AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue job is meant to be used for batch ETL data processing. It cannot be used to discover and protect your sensitive data in AWS.

Amazon Polly - Amazon Polly is a service that turns text into lifelike speech, allowing you to create applications that talk, and build entirely new categories of speech-enabled products. Polly's Text-to-Speech (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech. It cannot be used to discover and protect your sensitive data in AWS.

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. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. It cannot be used to discover and protect your sensitive data in AWS.

Reference:

https://aws.amazon.com/macie/

Domain
Technology

Question 28

A company wants to improve the resiliency of its flagship application so it wants to move from its traditional database system to a managed AWS NoSQL database service to support active-active configuration in both the East and West US AWS regions. The active-active configuration with cross-region support is the prime criteria for any database solution that the company considers.

Which AWS database service is the right fit for this requirement?

1] Amazon Aurora with multi-master clusters

2] Amazon DynamoDB with global tables

3] Amazon Relational Database Service (Amazon RDS) for MYSQL

4] Amazon DynamoDB with DynamoDB Accelerator

Overall explanation

Correct option:

Amazon DynamoDB with global tables

Amazon DynamoDB is a fully managed, serverless, key-value NoSQL database designed to run high-performance applications at any scale. DynamoDB offers built-in security, continuous backups, automated multi-region replication, in-memory caching, and data export tools.

DynamoDB global tables replicate data automatically across your choice of AWS Regions and automatically scale capacity to accommodate your workloads. With global tables, your globally distributed applications can access data locally in the selected regions to get single-digit millisecond read and write performance. DynamoDB offers active-active cross-region support that is needed for the company.

Incorrect options:

Amazon DynamoDB with DynamoDB Accelerator - DynamoDB Accelerator (DAX) is an in-memory cache that delivers fast read performance for your tables at scale by enabling you to use a fully managed in-memory cache. Using DAX, you can improve the read performance of your DynamoDB tables by up to 10 times—taking the time required

for reads from milliseconds to microseconds, even at millions of requests per second. DAX does not offer active-active cross-Region configuration.

Amazon Aurora with multi-master clusters - Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications. In a multi-master cluster, all DB instances have read/write capability. Aurora is not a NoSQL database, so this option is incorrect.

Amazon Relational Database Service (Amazon RDS) for MYSQL - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need. RDS is not a NoSQL database, so this option is incorrect.

References:

https://aws.amazon.com/dynamodb/features/

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-multi-master.html

Domain
Technology

Question 29
Which AWS services can be used to decouple components of a microservices based application on AWS Cloud? (Select two)

1] AWS Lambda
2] Amazon Simple Notification Service (SNS)
3] Amazon Elastic Compute Cloud (Amazon EC2)
4] AWS Step Functions
5] Amazon Simple Queue Service (SQS)

Overall explanation

Correct options:

Amazon Simple Queue Service (SQS)

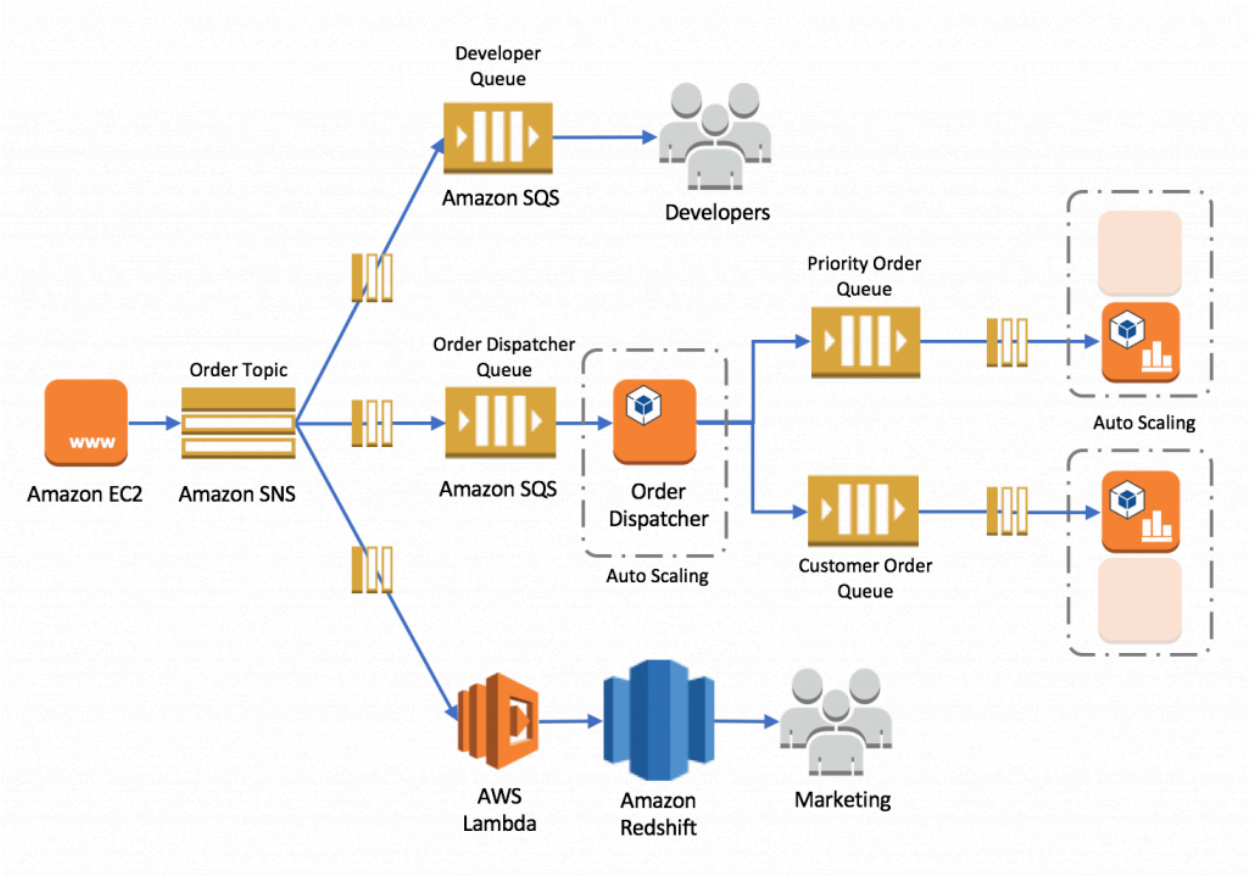
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

Amazon Simple Notification Service (SNS)

Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Using Amazon SNS topics, your publisher systems can fan-out messages to a large number of subscriber endpoints for parallel processing, including Amazon SQS queues, AWS Lambda functions, and HTTP/S webhooks. Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

Therefore, both SNS and SQS can be used to decouple components of a microservices-based application.

Please review this reference architecture for building a decoupled order processing system using SNS and SQS:



via - https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-amazon-sns/

Incorrect options:

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS. EC2 cannot be used to decouple components of a microservices-based application.

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Lambda cannot be used to decouple components of a microservices-based application.

AWS Step Functions - AWS Step Functions lets you coordinate multiple AWS services into serverless workflows. You can design and run workflows that stitch together services such as AWS Lambda, AWS Glue and Amazon SageMaker. AWS Step Functions cannot be used to decouple components of a microservices-based application.

Reference:

https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-amazon-sns/

https://aws.amazon.com/microservices/

Domain
Technology

Question 30
An intern at an IT company provisioned a Linux based On-demand EC2 instance with per-second billing but terminated it within 30 seconds as he wanted to provision another instance type. What is the duration for which the instance would be charged?

1] 30 seconds
2] 300 seconds
3] 60 seconds
4] 600 seconds

Overall explanation
Correct option:

60 seconds

There is a one-minute minimum charge for Linux based EC2 instances, so this is the correct option.

Incorrect options:

30 seconds

300 seconds

600 seconds

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

Reference:

https://aws.amazon.com/blogs/aws/new-per-second-billing-for-ec2-instances-and-ebs-volumes/

Domain
Billing and Pricing

Question 31
A web application stores all of its data on Amazon S3 buckets. A client has mandated that data be encrypted before sending it to Amazon S3.

Which of the following is the right technique for encrypting data as needed by the customer?

1] Enable client-side encryption using AWS encryption SDK
2] Enable server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS)
3] Encryption is enabled by default for all the objects written to Amazon S3. Additional configuration is not required
4] Enable server-side encryption with Amazon S3 Managed Keys (SSE-S3)

Overall explanation
Correct option:

Enable client-side encryption using AWS encryption SDK

The act of encrypting data before sending it to Amazon S3 is termed as client-side encryption. The AWS encryption SDK is a client-side encryption library that is separate from the language–specific SDKs. You can use this encryption library to more easily implement encryption best practices in Amazon S3. Unlike the Amazon S3 encryption clients in the language–specific AWS SDKs, the AWS encryption SDK is not tied to Amazon S3 and can be used to encrypt or decrypt data to be stored anywhere.

Incorrect options:

Enable server-side encryption with Amazon S3 Managed Keys (SSE-S3) - When you use server-side encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a root key that it regularly rotates.

Enable server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS) - Server-side encryption with AWS KMS keys (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a KMS key that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your KMS key was used and by whom.

Server-side encryption is the encryption of data at its destination by the application or service that receives it. Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. Hence, server-side encryption is not the right answer for the current scenario. So both these options are incorrect.

Encryption is enabled by default for all the objects written to Amazon S3. Additional configuration is not required - Although it's correct that encryption is enabled by default for all the objects written to Amazon S3, however, the given use case mandates that data be encrypted before sending it to Amazon S3, which cannot be accomplished with the given option. So this option is incorrect.

References:

https://docs.aws.amazon.com/en_us/AmazonS3/latest/userguide/UsingClientSideEncryption.html

https://docs.aws.amazon.com/en_us/AmazonS3/latest/userguide/serv-side-encryption.html

Domain
Security and Compliance

Question 32
Which security service of AWS is enabled for all AWS customers, by default, at no additional cost?
1] AWS Shield Standard
2] AWS Web Application Firewall (AWS WAF)
3] AWS Secrets Manager
4] AWS Shield Advanced

Overall explanation
Correct option:

AWS Shield Standard

AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications. While AWS Shield Standard helps protect all AWS customers, you get better protection if you are using Amazon CloudFront and Amazon Route 53. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge.

Incorrect options:

AWS Web Application Firewall (AWS WAF) - AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to an Amazon CloudFront distribution, an Amazon API Gateway API, or an Application Load Balancer. AWS WAF charges based on the number of web access control lists (web ACLs) that you create, the number of rules that you add per web ACL, and the number of web requests that you receive (it is not a free service).

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. With Secrets Manager, you pay based on the number of secrets stored and API calls made.

AWS Shield Advanced - AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer

4) attacks but also for application layer (layer 7) attacks. AWS Shield Advanced is a paid service that provides additional protections for internet-facing applications.

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

Domain
Security and Compliance

Question 33
A data analytics company is running a proprietary batch analytics application on AWS and wants to use a storage service which would be accessed by hundreds of EC2 instances simultaneously to append data to existing files. As a Cloud Practitioner, which AWS service would you suggest for this use-case?

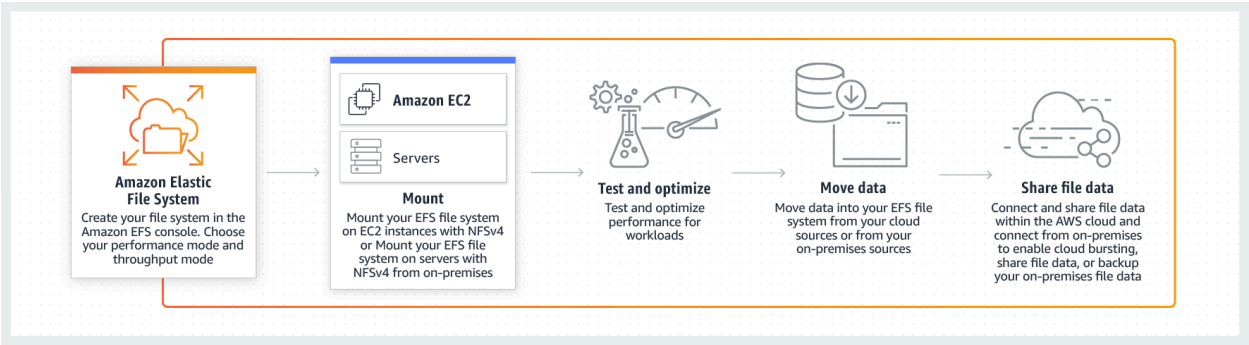
1] Amazon Elastic File System (Amazon EFS)
2] Instance Store
3] Amazon Simple Storage Service (Amazon S3)
4] Amazon Elastic Block Store (Amazon EBS)

Overall explanation
Correct option:

Amazon Elastic File System (Amazon EFS)

Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics, and concurrently-accessible storage for up to thousands of Amazon EC2 instances. Amazon EFS uses the Network File System protocol.

How EFS works:



via - https://aws.amazon.com/efs/

Incorrect options:

Amazon Elastic Block Store (Amazon EBS) - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. EBS volumes cannot be accessed simultaneously by multiple EC2 instances, so this option is incorrect.

Instance Store - An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance Store volumes cannot be accessed simultaneously by multiple EC2 instances, so this option is incorrect.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 is object storage and it does not support file append operations, so this option is incorrect.

Reference:

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

Domain
Technology

Question 34 Correct

Compared to the on-demand instance prices, what is the highest possible discount offered for spot instances?

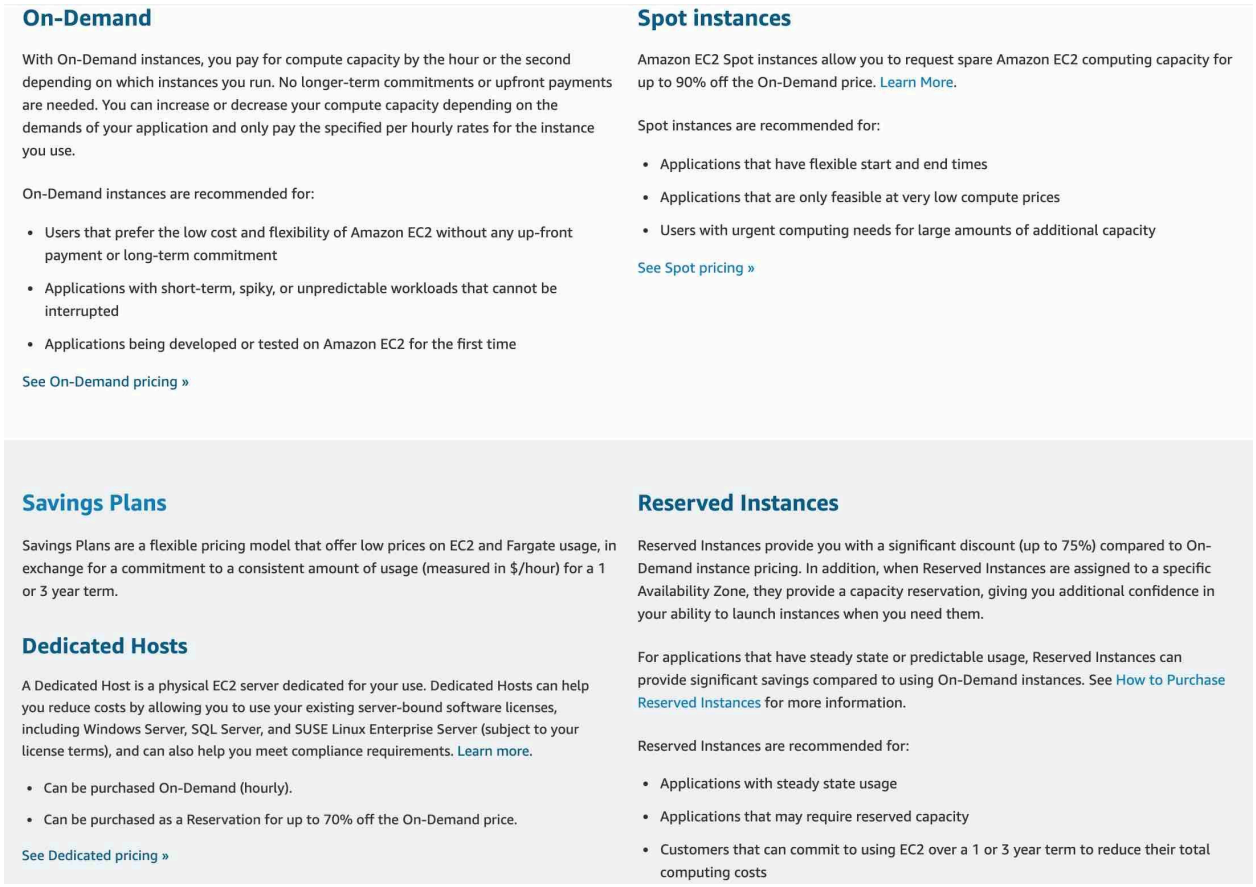
1] 50
2] 90
3] 10
4] 75

Overall explanation
Correct option:

90

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 the on-demand instance prices. You can use spot instances for various stateless, fault-tolerant, or flexible applications such as big data, containerized workloads, CI/CD, web servers, high-performance computing (HPC), and other test & development workloads.

EC2 Pricing Options Overview:



via - https://aws.amazon.com/ec2/pricing/

Incorrect options:

75

10

50

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

Reference:

https://aws.amazon.com/ec2/spot/

Domain
Technology

Question 35

According to the AWS Cloud Adoption Framework (AWS CAF), what are two tasks that a company should perform when planning to migrate to the AWS Cloud and aiming to become more responsive to customer inquiries and feedback as part of their organizational transformation? (Select two)

1] Create new analytical insights with existing products and services

2] Organize your teams around products and value streams

3] Leverage legacy infrastructure for cost efficiencies

4] Organize your teams around bureaucratic design principles

5] Leverage agile methods to rapidly iterate and evolve

Overall explanation

Correct options:

The AWS Cloud Adoption Framework (AWS CAF) leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations. These capabilities provide best practice guidance that helps you improve your cloud readiness. AWS CAF groups its capabilities in six perspectives: Business, People, Governance, Platform, Security, and Operations.

Organize your teams around products and value streams

Leverage agile methods to rapidly iterate and evolve

Using the AWS Cloud Adoption Framework (AWS CAF), you can reimagine how your business and technology teams create customer value and meet your strategic intent. Organizing your teams around products and value streams while leveraging agile methods to rapidly iterate and evolve will help you become more responsive and customer centric.

Incorrect options:

Leverage legacy infrastructure for cost efficiencies

Create new analytical insights with existing products and services

Organize your teams around bureaucratic design principles

These three options are not in agreement with the tasks outlined by the AWS Cloud Adoption Framework (AWS CAF) to become more responsive to customer inquiries and feedback, hence these options are incorrect.

Reference:

https://aws.amazon.com/cloud-adoption-framework/

Domain
Cloud Concepts

Question 36
Which AWS Route 53 routing policy would you use to route traffic to multiple resources and also choose how much traffic is routed to each resource?

1] Weighted routing
2] Simple routing
3] Failover routing
4] latency-based routing

Overall explanation
Correct option:

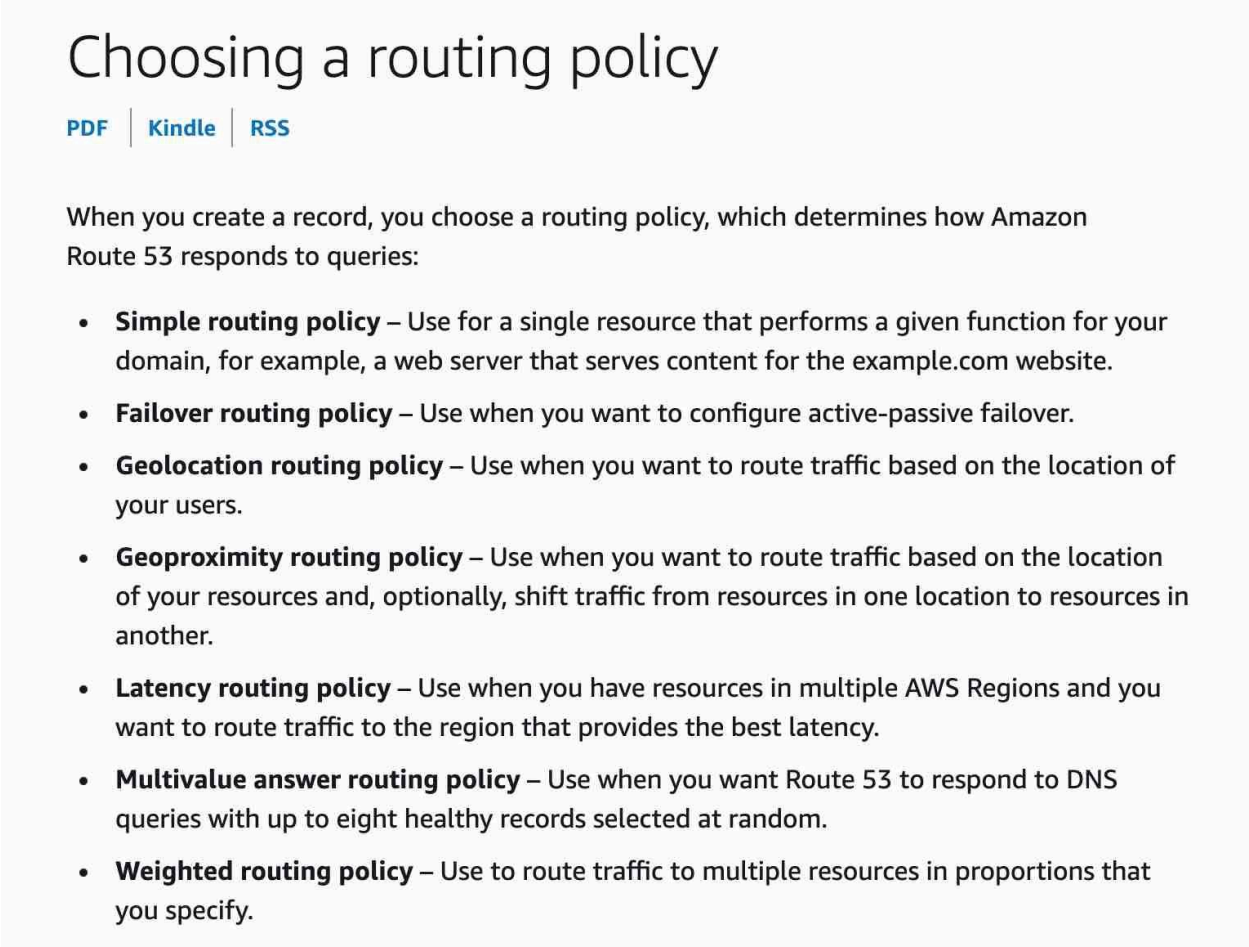
Weighted routing

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.

Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load

balancing and testing new versions of software. To configure weighted routing, you create records that have the same name and type for each of your resources. You assign each record a relative weight that corresponds with how much traffic you want to send to each resource. Amazon Route 53 sends traffic to a resource based on the weight that you assign to the record as a proportion of the total weight for all records in the group.

Route 53 Routing Policy Overview:



Choosing a routing policy

PDF | Kindle | RSS

When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries:

- **Simple routing policy** – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
- **Failover routing policy** – Use when you want to configure active-passive failover.
- **Geolocation routing policy** – Use when you want to route traffic based on the location of your users.
- **Geoproximity routing policy** – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
- **Latency routing policy** – Use when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.
- **Multivalue answer routing policy** – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
- **Weighted routing policy** – Use to route traffic to multiple resources in proportions that you specify.

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

Incorrect options:

Failover routing - This routing policy is used when you want to configure active-passive failover.

Simple routing - With simple routing, you typically route traffic to a single resource, for example, to a web server for your website.

latency-based routing - This routing policy is used when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.

Reference:

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

Domain
Technology

Question 37
What are the advantages that AWS Cloud offers over a traditional on-premises IT infrastructure? (Select two)

1] Provide lower latency to applications by maintaining servers on-premises
2] Eliminate guessing on your infrastructure capacity needs
3] Increase speed and agility by keeping servers and other required resources ready before time in your data centers
4] Make a capacity decision before deploying an application, to reduce costs
5] Trade capital expense for variable expense

Overall explanation
Correct options:

Trade capital expense for variable expense

In a traditional on-premises environment, you have to invest heavily in data centers and servers before you know how you're going to use them. With Cloud Computing, you can pay only when you consume computing resources, and pay only for how much you consume.

Eliminate guessing on your infrastructure capacity needs

When you make a capacity decision before deploying an application, you often end up either sitting on expensive idle resources or dealing with limited capacity. With Cloud Computing, these problems go away. 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. You can Stop guessing capacity.

Incorrect options:

Make a capacity decision before deploying an application, to reduce costs - As explained above, when you make a capacity decision before deploying an application, you often end up either sitting on expensive idle resources or dealing with limited capacity.

Provide lower latency to applications by maintaining servers on-premises - Maintaining servers on-premises involves costly capital expenses and costly ongoing expenses to maintain, manage and upgrade them.

Increase speed and agility by keeping servers and other required resources ready before time in your data centers - This again is indicative of maintaining on-premises infrastructure which is neither a cost-effective or time effective way of managing the resources.

Reference:

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

Domain
Cloud Concepts

Question 38
Which of the following AWS services support VPC Endpoint Gateway for a private connection from a VPC? (Select two)
1] Amazon Simple Storage Service (Amazon S3)
2] Amazon Elastic Compute Cloud (Amazon EC2)
3] Amazon Simple Notification Service (SNS)
4] Amazon Simple Queue Service (SQS)
5] Amazon DynamoDB

Overall explanation
Correct options:

Amazon Simple Storage Service (Amazon S3)

Amazon DynamoDB

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

There are two types of VPC endpoints: interface endpoints and gateway endpoints.

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses.

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:

Amazon Simple Storage Service (Amazon S3)

Amazon DynamoDB

Exam Alert:

You may see a question around this concept in the exam. Just remember that only Amazon S3 and Amazon DynamoDB support VPC gateway endpoint. All other services that support VPC Endpoints use a VPC interface endpoint (note that Amazon S3 supports the VPC interface endpoint as well).

Incorrect options:

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Simple Queue Service (SQS)

Amazon Simple Notification Service (SNS)

As explained earlier, these services support VPC Endpoint Interfaces.

Reference:

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

Domain
Security and Compliance

Question 39
A medical research startup wants to understand the compliance of AWS services concerning HIPAA guidelines. Which AWS service can be used to review the HIPAA compliance and governance-related documents on AWS?

1] AWS Secrets Manager
2] AWS Systems Manager
3] AWS Trusted Advisor
4] AWS Artifact

Overall explanation
Correct option:

AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to your organization. It provides on-demand access to AWS security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Different types of agreements are available in AWS Artifact Agreements to address the needs of customers subject to specific regulations. For example, the Business Associate Addendum (BAA) is available for customers that need to comply with the Health Insurance Portability and Accountability Act (HIPAA). It is not a service, it's a no-cost, self-service portal for on-demand access to AWS compliance reports.

Incorrect options:

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. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally.

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. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources.

Reference:

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

Domain
Security and Compliance

Question 40
Which AWS service will help you receive alerts when the reservation utilization falls below the defined threshold?

1] AWS Trusted Advisor
2] AWS Pricing Calculator
3] AWS Budgets
4] AWS CloudTrail

Overall explanation

Correct option:

AWS Budgets

AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.

You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Reservation alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon Elasticsearch reservations.

Incorrect options:

AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You cannot use this service to receive alerts when the reservation utilization falls below the defined threshold.

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With AWS CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. AWS 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. You cannot use this service to receive alerts when the reservation utilization falls below the defined threshold.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by AWS Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost

Optimization, Performance, Security, Fault Tolerance, Service Limits. You cannot use this service to receive alerts when the reservation utilization falls below the defined threshold.

References:

https://aws.amazon.com/aws-cost-management/aws-budgets/

https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/

Domain
Billing and Pricing

Question 41

Which type of cloud computing does Amazon Elastic Compute Cloud (EC2) represent?

1] Network as a Service (NaaS)
2] Infrastructure as a Service (IaaS)
3] Software as a Service (SaaS)
4] Platform as a Service (PaaS)

Overall explanation
Correct option:

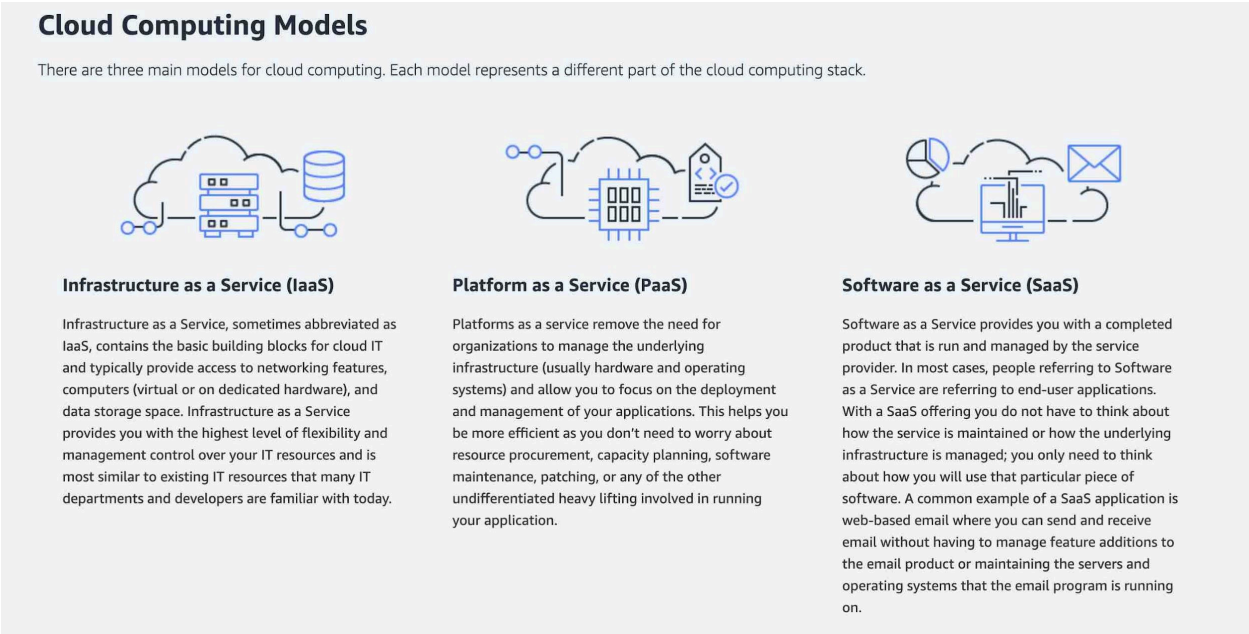
Infrastructure as a Service (IaaS)

Cloud Computing can be broadly divided into three types - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

IaaS contains the basic building blocks for cloud IT. It typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS gives the highest level of flexibility and management control over IT resources.

EC2 gives you full control over managing the underlying OS, virtual network configurations, storage, data and applications. So EC2 is an example of an IaaS service.

Please review this overview of the types of Cloud Computing:



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

Incorrect options:

Platform as a Service (PaaS) - PaaS removes the need to manage underlying infrastructure (usually hardware and operating systems), and allows you to focus on the deployment and management of your applications. 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.

Elastic Beanstalk is an example of a PaaS service. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.

Software as a Service (SaaS) - SaaS provides you with a complete product that is run and managed by the service provider. With a SaaS offering, you don't 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 software. AWS Rekognition is an example of a SaaS service.

Network as a Service (NaaS) - This is a made-up option and has been added as a distractor.

Reference:

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

Domain
Cloud Concepts

Question 42
A company wants to move to AWS cloud and release new features with quick iterations by utilizing relevant AWS services whenever required. Which of the following characteristics of AWS Cloud does it want to leverage?

1] Scalability

2] Elasticity

3] Reliability

4] Agility

Overall explanation
Correct option:

Agility

In the world of cloud computing, "Agility" refers to the ability to rapidly develop, test and launch software applications that drive business growth Another way to explain "Agility" - AWS provides a massive global cloud infrastructure that allows you to quickly innovate, experiment and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications. This ability is called Agility.

Incorrect options:

Elasticity - This refers to the ability to acquire resources as you need and release when they are no longer needed is termed as Elasticity of the Cloud.

Reliability - This refers to the ability of a system to recover from infrastructure or service disruptions, by dynamically acquiring computing resources to meet demand, and mitigate disruptions.

Scalability - Scalability is the measurement of a system's ability to grow to accommodate an increase in demand, or shrink down to a diminishing demand.

Reference:

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

https://wa.aws.amazon.com/wat.concepts.wa-concepts.en.html

Domain
Cloud Concepts

Question 43
AWS Shield Advanced provides expanded DDoS attack protection for web applications running on which of the following resources? (Select two)

1] AWS Global Accelerator

2] AWS CloudFormation

3] Amazon Route 53

4] AWS Elastic Beanstalk

5] Amazon API Gateway

Overall explanation
Correct options:

Amazon Route 53

AWS Global Accelerator

AWS Shield Standard is activated for all AWS customers, by default. For higher levels of protection against attacks, you can subscribe to AWS Shield Advanced. With Shield Advanced, you also have exclusive access to advanced, real-time metrics and reports for extensive visibility into attacks on your AWS resources. With the assistance of the DRT (DDoS response team), AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks but also for application layer (layer 7) attacks.

AWS Shield Advanced provides expanded DDoS attack protection for web applications running on the following resources: Amazon Elastic Compute Cloud, Elastic Load Balancing (ELB), Amazon CloudFront, Amazon Route 53, AWS Global Accelerator.

Incorrect options:

Amazon API Gateway - Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Amazon Web Application Firewall is used to monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API. It is not covered under AWS Shield Advanced.

AWS CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. CloudFormation is not covered under AWS Shield Advanced.

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with various programming languages. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Elastic Beanstalk is covered under AWS Shield Standard. Advanced coverage is not offered for this service.

Reference:
https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html

Domain
Security and Compliance

Question 44
A startup wants to set up its IT infrastructure on AWS Cloud. The CTO would like to get an estimate of the monthly AWS bill based on the AWS services that the startup wants to use. As a Cloud Practitioner, which AWS service would you suggest for this use-case?

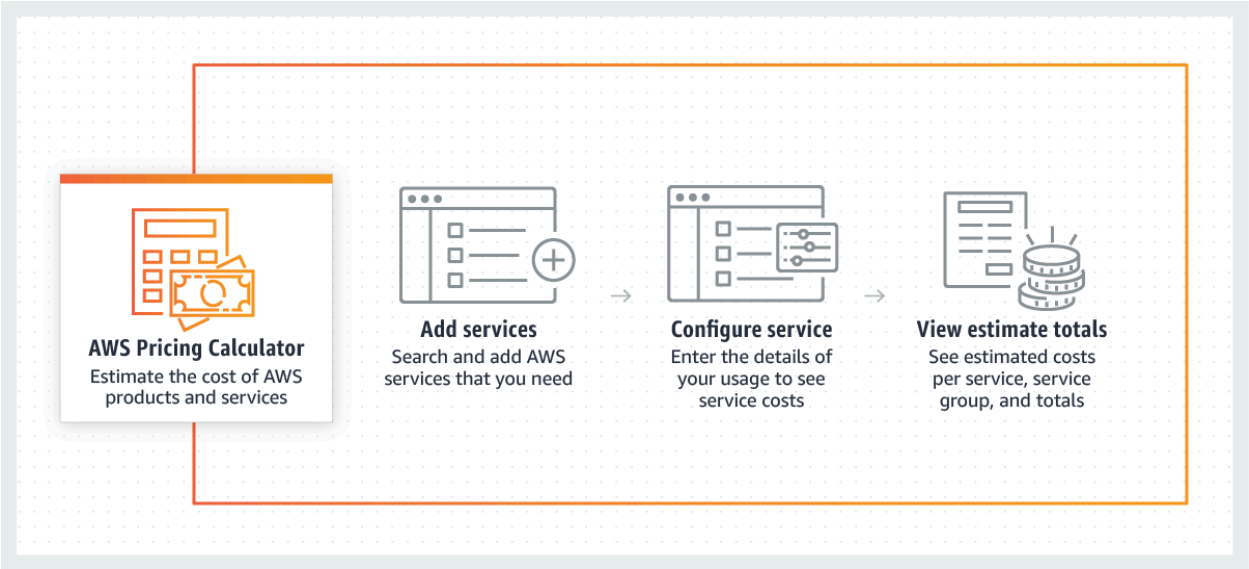
1] AWS Pricing Calculator
2] AWS Cost Explorer
3] AWS Budgets
4] AWS Cost & Usage Report (AWS CUR)

Overall explanation

Correct option:

AWS Pricing Calculator

AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services. AWS Pricing Calculator can provide the estimate of the AWS service usage based on the list of AWS services.



via - https://calculator.aws/#/

The AWS Pricing Calculator is accessible on : https://calculator.aws/#/

You should also note AWS is in the process of deprecating a similar tool called the Simple Monthly Calculator. This calculator provides an estimate of usage charges for AWS services based on certain information you provide. It helps customers and prospects estimate their monthly AWS bill more efficiently. This tool can be accessed on : https://calculator.s3.amazonaws.com/index.html

Incorrect options:

AWS Cost & Usage Report (AWS CUR) - The AWS Cost & Usage Report (AWS CUR) contains the most comprehensive set of AWS cost and usage data available, including additional metadata about AWS services, pricing, credit, fees, taxes, discounts, cost categories, Reserved Instances, and Savings Plans. The AWS Cost & Usage Report (AWS CUR) itemizes usage at the account or Organization level by product code, usage type and operation. These costs can be further organized by Cost Allocation tags and Cost Categories. The AWS Cost & Usage Report (AWS CUR) is available at an hourly, daily, or monthly level of granularity, as well as at the management or member account level. The AWS Cost & Usage Report (AWS CUR) cannot provide the estimate of the monthly AWS bill based on the list of AWS services.

AWS Cost Explorer - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and gives you a detailed breakdown of all services in the table view. The reports let you adjust the time range to view historical data going back up to twelve months to gain an understanding of your cost trends. AWS Cost Explorer cannot provide the estimate of the monthly AWS bill based on the list of AWS services.

AWS Budgets - AWS Budgets gives the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Budgets can be created at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. AWS Budgets cannot provide the estimate of the monthly AWS bill based on the list of AWS services.

Reference:

https://calculator.aws/#/

Domain
Billing and Pricing

Question 45

Under the AWS Shared Responsibility Model, which of the following is a shared responsibility of both AWS and the customer?

1] Availability Zone (AZ) infrastructure maintenance

2] Infrastructure maintenance of Amazon Simple Storage Service (Amazon S3) storage servers

3] Guarantee data separation among various AWS customers

4] Configuration Management

Overall explanation

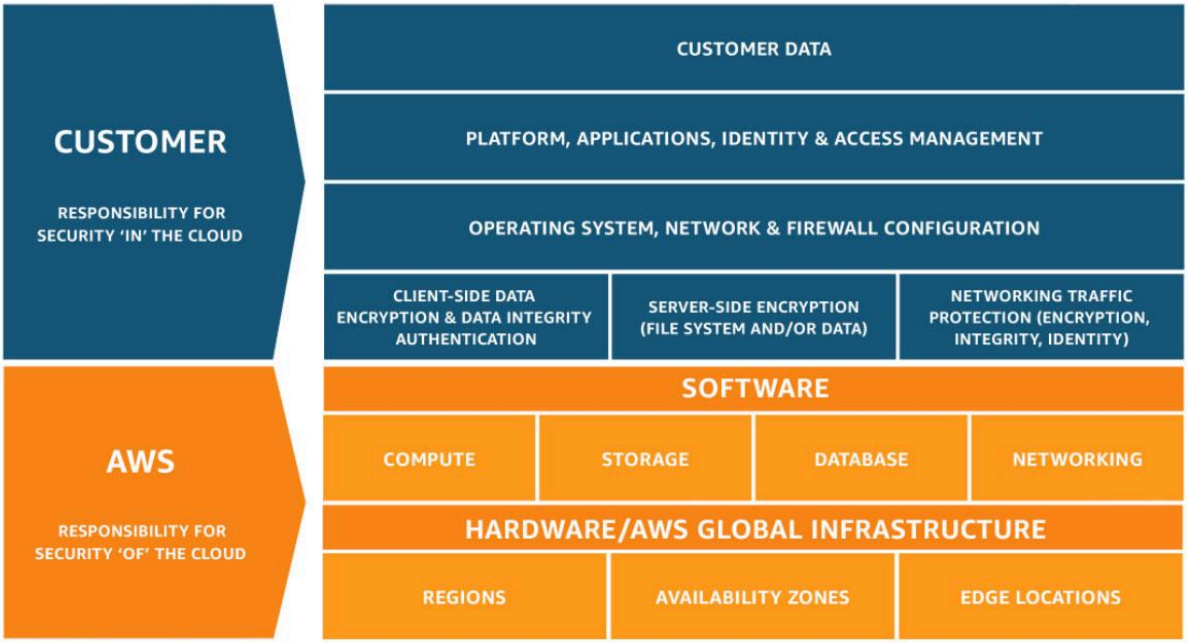
Correct option:

Configuration Management

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.

Controls that apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives are called shared controls. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Configuration Management forms a part of shared controls - AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

Shared Responsibility Model Overview:



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

Incorrect options:

Infrastructure maintenance of Amazon Simple Storage Service (Amazon S3) storage servers - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.

Guarantee data separation among various AWS customers - 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.

Availability Zone (AZ) infrastructure maintenance - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.

Reference:

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

Domain
Security and Compliance

Question 46

Which of the following Amazon S3 storage classes takes the most time to retrieve data (also known as first byte latency)?

1] Amazon S3 Standard

2] Amazon S3 Glacier Flexible Retrieval

3] Amazon S3 Intelligent-Tiering

4] Amazon S3 Glacier Deep Archive

Overall 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 in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. Amazon S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases. It has a retrieval time (first byte latency) of 12 to 48 hours.

Please review this illustration for Amazon S3 Storage Classes data retrieval times. You don't need to memorize the actual numbers, just remember that Amazon S3 Glacier Deep Archive takes the most time to retrieve data:

Performance across the S3 Storage Classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	40 KB	40 KB
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

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

Incorrect options:

Amazon S3 Standard - Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Amazon S3 Standard has a retrieval time (first byte latency) of milliseconds.

Amazon S3 Intelligent-Tiering - The Amazon S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. Amazon S3 Intelligent-Tiering has a retrieval time (first byte latency) of milliseconds.

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.

Reference:

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

Domain
Technology

Question 47
Which of the following is a serverless AWS service?

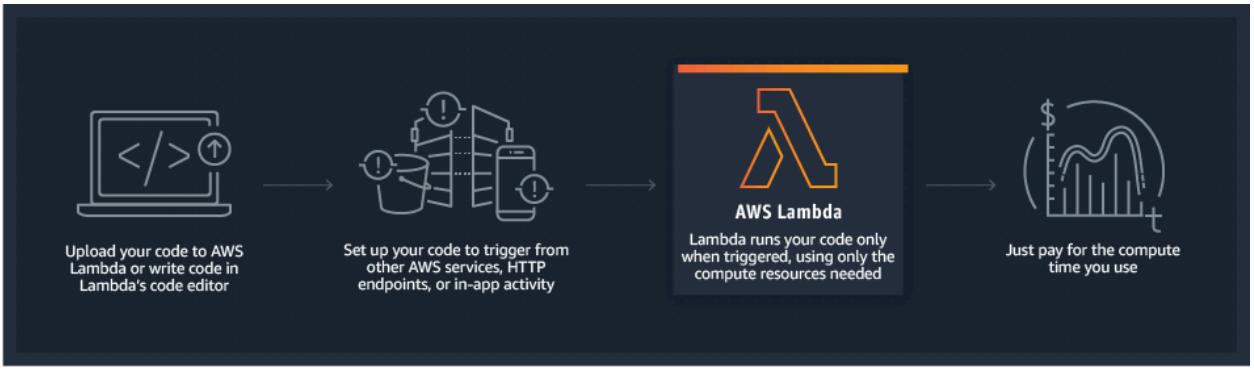
1] AWS Lambda
2] Amazon Elastic Compute Cloud (Amazon EC2)
3] Amazon EMR
4] AWS Elastic Beanstalk
5] Overall explanation

Correct option:

AWS Lambda

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability.

How Lambda Works:



via - https://aws.amazon.com/lambda/

Incorrect options:

Amazon Elastic Compute Cloud (Amazon EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS. EC2 is not a serverless service.

Amazon EMR - Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Hadoop, Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. Amazon EMR can be used to provision resources to run big data workloads on Hadoop clusters. Amazon EMR provisions EC2 instances to manage its workload. Amazon EMR is not a serverless service.

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. AWS Elastic Beanstalk provisions servers so it is not a serverless service.

Reference:

https://aws.amazon.com/lambda/

Domain
Technology

Question 48
Which of the following AWS services can be used to connect a company's on-premises environment to a VPC without using the public internet?

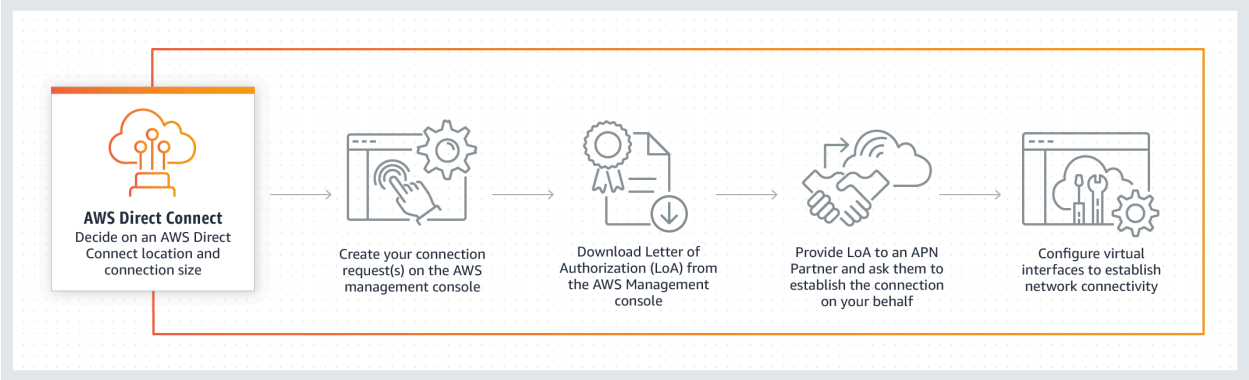
1] AWS Direct Connect
2] AWS Site-to-Site VPN
3] Internet Gateway
4] VPC Endpoint

Overall explanation
Correct option:

AWS Direct Connect

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you with a private, high bandwidth network connection between your network and your VPC. This connection is private and does not go over the public internet. It takes at least a month to establish this physical connection.

How Direct Connect Works:



via - https://aws.amazon.com/directconnect/

Incorrect options:

VPC Endpoint - A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. VPC Endpoint cannot be used to privately connect on-premises data center to AWS Cloud.

Internet Gateway - An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for

instances. Internet Gateway cannot be used to privately connect on-premises data center to AWS Cloud.

AWS Site-to-Site VPN - AWS Site-to-Site VPN creates a secure connection between your data center or branch office and your AWS cloud resources. This connection goes over the public internet.

References:

https://aws.amazon.com/directconnect/

https://aws.amazon.com/vpn/

Domain
Cloud Concepts

Question 49

A company runs an application on a fleet of EC2 instances. The company wants to automate the traditional maintenance job of running timely assessments and checking for OS vulnerabilities. As a Cloud Practitioner, which service will you suggest for this use case?

1] Amazon GuardDuty
2] Amazon Inspector
3] Amazon Macie
4] AWS Shield
5] Overall explanation

Correct option:

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on your Amazon EC2 instances. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These

findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Incorrect options:

Amazon GuardDuty - Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). This service is for AWS account level access, not for instance-level management like an EC2. GuardDuty cannot be used to check OS vulnerabilities.

Amazon Macie - Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII). This service is for securing data and has nothing to do with an EC2 security assessment. Macie cannot be used to check OS vulnerabilities.

AWS Shield - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. Shield is general protection against DDos attacks for all resources in the AWS network, and not an instance-level security assessment service. Shield cannot be used to check OS vulnerabilities.

Reference:

https://aws.amazon.com/inspector/

Domain
Security and Compliance

Question 50

Which of the following AWS Support plans provide access to guidance, configuration, and troubleshooting of AWS interoperability with third-party software? (Select two)

1] AWS Corporate Support
2] AWS Basic Support
3] AWS Enterprise Support
4] AWS Business Support
5] AWS Developer Support

Overall explanation

Correct options:

AWS Enterprise Support

AWS Enterprise Support provides customers with concierge-like service where the main focus is helping the customer achieve their outcomes and find success in the cloud. With Enterprise Support, you get 24x7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative architectural guidance delivered in the context of your applications and use-cases, and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts. You get access to guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

AWS Business Support

You should use AWS Business Support if you have production workloads on AWS and want 24x7 phone, email and chat access to technical support and architectural guidance in the context of your specific use-cases. You get full access to AWS Trusted Advisor Best Practice Checks. You get access to guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

Exam Alert:

Please review the differences between the AWS Developer Support, AWS Business Support, AWS Enterprise On-Ramp Support and AWS Enterprise Support plans as you can expect at least a couple of questions on the exam:

	Developer	Business	Enterprise On-Ramp	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Minimum recommended tier if you have production workloads in AWS*	*Recommended if you have production and/or business critical workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
AWS Trusted Advisor Best Practice Checks	Service Quota and basic Security checks	Full set of checks	Full set of checks	Full set of checks
AWS Trusted Advisor Priority				Prioritized recommendations curated by your AWS account team
Enhanced Technical Support	Business hours** web access to Cloud Support Associates Unlimited cases with 1 primary contact Prioritized responses on AWS re:Post	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack
Case Severity / Response Times*	General guidance: < 24 hours** System impaired: < 12 hours**	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 30 minutes	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business/Mission-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications (one-per-year)	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API	AWS Support API

	Developer *Recommended if you are experimenting or testing in AWS.*	Business *Minimum recommended tier if you have production workloads in AWS*	Enterprise On-Ramp *Recommended if you have production and/or business critical workloads in AWS.*	Enterprise *Recommended if you have business and/or mission critical workloads in AWS.*
Third-Party Software Support		Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting
Proactive Programs and Self Service	Access to Support Automation Workflows with prefixes AWSSupport	Access to Infrastructure Event Management for additional fee Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport	Infrastructure Event Management (one-per-year) Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport	Infrastructure Event Management Access to proactive reviews, workshops, and deep dives Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport
AWS Incident Detection and Response				Access to AWS Incident Detection and Response **for an additional fee**. AWS Incident Detection and Response is an add-on to Enterprise Support that offers 24x7 proactive monitoring and incident management for selected workloads. AWS Incident Detection and Response leverages the proven operational, enhanced monitoring, and incident management capabilities used internally by AWS teams and externally by AWS Managed Services (AMS).
AWS Managed Services		Access to AWS Managed Services (AMS) **for an additional fee**. AMS augments your existing teams with cloud advanced operations skills and capacity. Includes baseline operations, a designated Cloud Service Delivery Manager (CSDM), Cloud Architect (CA), and access to the AMS security team.	Access to AWS Managed Services (AMS) **for an additional fee**. AMS augments your existing teams with cloud advanced operations skills and capacity. Includes baseline operations, a designated Cloud Service Delivery Manager (CSDM), Cloud Architect (CA), and access to the AMS security team.	Access to AWS Managed Services (AMS) **for an additional fee**. AMS augments your existing teams with cloud operations skills and capacity. It includes baseline operations, a designated Cloud Service Delivery Manager (CSDM), Cloud Architect (CA), and access to the AMS security team. AWS Incident Detection and Response is available at no additional charge in eligible regions for AWS Managed Services direct customers with AWS Enterprise Support.

	Developer	Business	Enterprise On-Ramp	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Minimum recommended tier if you have production workloads in AWS*	*Recommended if you have production and/or business critical workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
Technical Account Management			A pool of Technical Account Managers to provide proactive guidance, and coordinate access to programs and AWS experts	Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization and coordinate access to programs and AWS experts
Training				Access to online self-paced labs
Account Assistance			Concierge Support Team	Concierge Support Team
Pricing *Additional services for **additional fee**	Greater of $29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of $100 / month*** - or - 10% of monthly AWS usage for the first $0–$10K 7% of monthly AWS usage from $10K–$80K 5% of monthly AWS usage from $80K–$250K 3% of monthly AWS usage over $250K See pricing detail and example. *Access to AWS Managed Services (AMS) **for an additional fee**	Greater of $5,500 - or - 10% of monthly AWS usage See pricing detail and example. *Access to AWS Managed Services (AMS) **for an additional fee**	Greater of $15,000 - or - 10% of monthly AWS usage for the first $0–$150K 7% of monthly AWS usage from $150K–$500K 5% of monthly AWS usage from $500K–$1M 3% of monthly AWS usage over $1M See pricing detail and example. * Access to AWS Incident Detection and Response **for an additional fee.** *Access to AWS Managed Services (AMS) **for an additional fee**

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

Incorrect options:

AWS Basic Support - The AWS Basic Support only provides access to the following:

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Health - Your Account Health Dashboard : A personalized view of the health of your AWS services, and alerts when your resources are impacted.

AWS Developer Support - You should use AWS Developer Support plan if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours. This plan also supports general guidance on how

services can be used for various use cases, workloads, or applications. You do not get access to Infrastructure Event Management with this plan.

Both these plans do not support access to guidance, configuration, and troubleshooting of AWS interoperability with third-party software.

AWS Corporate Support - This is a made-up option and has been added as a distractor.

Reference:

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

Domain
Billing and Pricing

Question 51

AWS Web Application Firewall (WAF) offers protection from common web exploits at which layer?

1] Layer 3
2] Layer 7
3] Layer 4
4] Layer 4 and 7
5] Overall explanation

Correct option:

Layer 7

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. HTTP and HTTPS requests are part of the Application layer, which is layer 7.

Incorrect options:

Layer 3 - Layer 3 is the Network layer and this layer decides which physical path data will take when it moves on the network. AWS Shield offers protection at this layer. WAF does not offer protection at this layer.

Layer 4 - Layer 4 is the Transport layer and this layer data transmission occurs using TCP or UDP protocols. AWS Shield offers protection at this layer. WAF does not offer protection at this layer.

Layer 4 and 7 - This option has been added as a distractor.

Reference:
https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

Domain
Security and Compliance

Question 52

The DevOps team at an e-commerce company is trying to debug performance issues for its serverless application built using a microservices architecture. As a Cloud Practitioner, which AWS service would you recommend addressing this use-case?

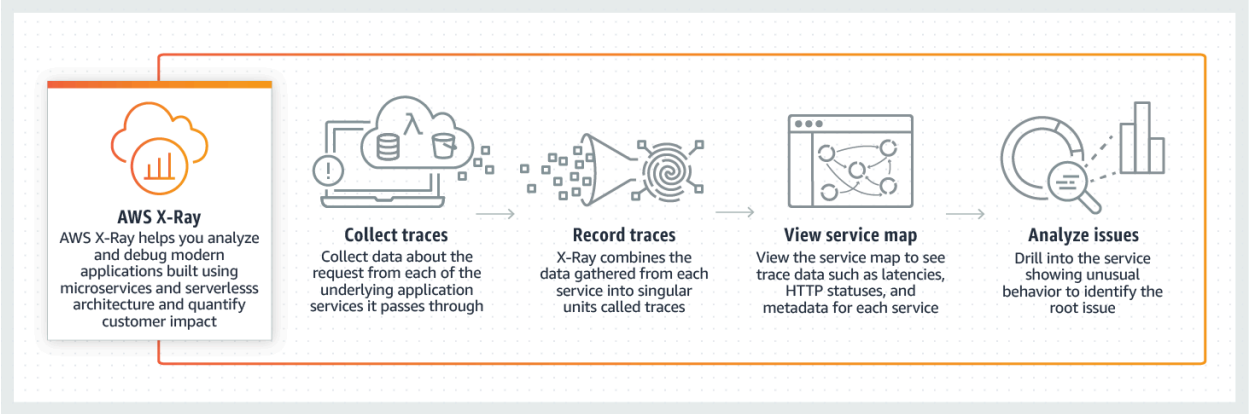
1] AWS Trusted Advisor
2] AWS X-Ray
3] AWS CloudFormation
4] Amazon Pinpoint
5] Overall explanation

Correct option:

AWS X-Ray

You can use AWS X-Ray to analyze and debug serverless and 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.

How AWS X-Ray Works:



via - https://aws.amazon.com/xray/

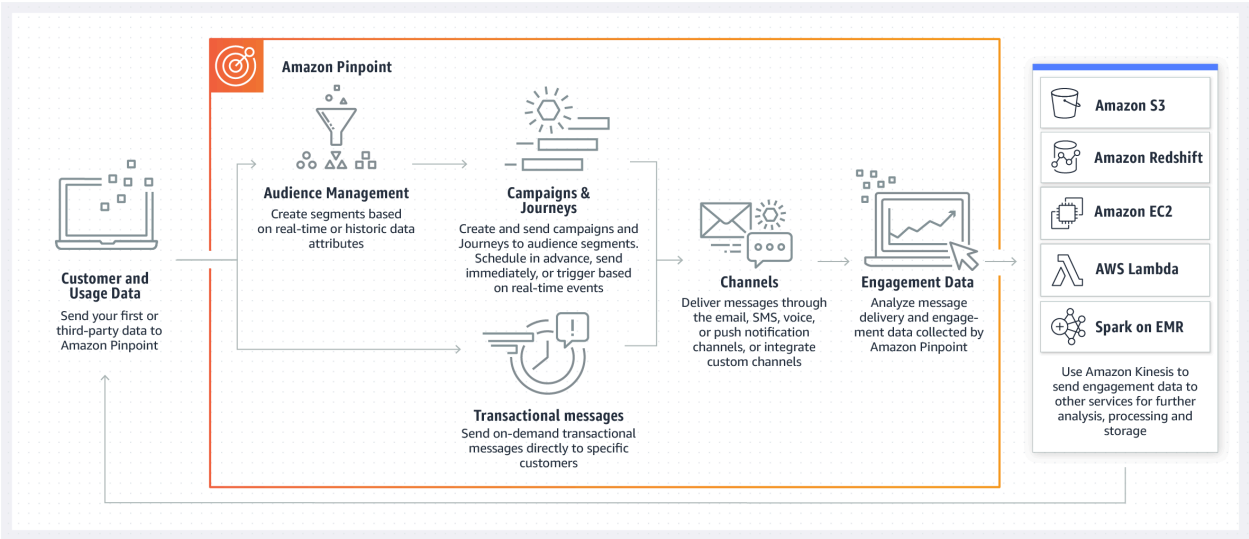
Incorrect options:

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 on cost optimization, security, fault tolerance, service limits and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. Trusted Advisor cannot be used to debug performance issues for this serverless application built using a microservices architecture.

Amazon Pinpoint - Amazon Pinpoint allows marketers and developers to deliver customer-centric engagement experiences by capturing customer usage data to draw real-time insights. Pinpoint cannot be used to debug performance issues for this serverless application built using a microservices architecture.

AWS CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. CloudFormation cannot be used to debug performance issues for this serverless application built using a microservices architecture.

How Amazon Pinpoint Works:



via - https://aws.amazon.com/pinpoint/

Reference:

https://aws.amazon.com/xray/

Domain
Technology

Question 53

Which of the following is a benefit of using AWS managed services such as Amazon Relational Database Service (Amazon RDS)?

1] The performance of AWS managed Amazon Relational Database Service (Amazon RDS) instance is better than a customer-managed database instance
2] There is no need to optimize database instance type and size
3] The customer needs to manage database backups
4] The customer needs to patch the underlying OS

Overall explanation
Correct option:

The performance of AWS managed Amazon Relational Database Service (Amazon RDS) instance is better than a customer-managed database instance

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups.

Amazon RDS provides a selection of instance types optimized to fit different relational database use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your database to optimize the database for your use-case by selecting the correct instance type and size.

As the RDS instances are optimized for memory, performance, or I/O, therefore the performance of AWS managed Amazon Relational Database Service (Amazon RDS) instance is better than a customer-managed database instance.

Incorrect options:

The customer needs to patch the underlying OS

The customer needs to manage database backups

There is no need to optimize database instance type and size

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

Reference:

https://aws.amazon.com/rds/instance-types/

Domain
Cloud Concepts

Question 54

The DevOps team at an IT company is moving 500 GB of data from an EC2 instance to an S3 bucket in the same region. Which of the following scenario captures the correct charges for this data transfer?

1] The company would only be charged for the outbound data transfer from EC2 instance

2] The company would only be charged for the inbound data transfer into the S3 bucket

3] The company would not be charged for this data transfer

4] The company would be charged for both the outbound data transfer from EC2 instance as well as the inbound data transfer into the S3 bucket

Overall explanation

Correct option:

The company would not be charged for this data transfer

There are three fundamental drivers of cost with AWS: compute, storage, and outbound data transfer. In most cases, there is no charge for inbound data transfer or data transfer between other AWS services within the same region. Outbound data transfer is aggregated across services and then charged at the outbound data transfer rate.

Per AWS pricing, data transfer between S3 and EC2 instances within the same region is not charged, so there would be no data transfer charge for moving 500 GB of data from an EC2 instance to an S3 bucket in the same region.

Incorrect options:

The company would only be charged for the outbound data transfer from EC2 instance

The company would only be charged for the inbound data transfer into the S3 bucket

The company would be charged for both the outbound data transfer from EC2 instance as well as the inbound data transfer into the S3 bucket

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

References:

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

https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf

Domain
Billing and Pricing

Question 55
Which of the following is the MOST cost-effective option to purchase an EC2 Reserved Instance (RI)?

1] All upfront payment option with the standard 1-year term
2] Partial upfront payment option with standard 3-years term
3] No upfront payment option with standard 3-years term
4] No upfront payment option with standard 1-year term

Overall explanation
Correct option:

Partial upfront payment option with standard 3-years term

You can use Amazon EC2 Reserved Instances (RI) to reserve capacity and receive a discount on your instance usage compared to running On-Demand instances. The discounted usage price is reserved for the duration of your contract, allowing you to predict compute costs over the term of the Reserved Instance (RI).

Please review this pricing comparison for EC2 Reserved Instances (RI):

Standard 1-Year Term

Payment Option	Upfront	Monthly*	Effective Hourly	Savings over On-Demand	On-Demand Hourly
No Upfront	$0	$44.53	$0.061	36%	$0.096 per Hour
Partial Upfront	$256	$21.17	$0.058	39%	
All Upfront	$501	$0	$0.057	40%	

Standard 3-Year Term

Payment Option	Upfront	Monthly*	Effective Hourly	Savings over On-Demand
No Upfront	$0	$30.66	$0.042	56%
Partial Upfront	$515	$14.60	$0.040	59%
All Upfront	$968	$0	$0.037	62%

via - https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf

So the percentage savings for each option is as follows:

"No upfront payment option with the standard 1-year term" - 36%

"All upfront payment option with the standard 1-year term" - 40%

"No upfront payment option with the standard 3-years term" - 56%

"Partial upfront payment option with the standard 3-years term" - 59%

Exam Alert:

For the exam, there is no need to memorize these savings numbers. All you need to remember is that a 3 years term would always be more cost-effective than a 1-year term. Then within a term, "all upfront" is better than "partial upfront" which in turn is better than "no upfront" from a cost savings perspective.

Incorrect options:

All upfront payment option with the standard 1-year term

No upfront payment option with standard 1-year term

No upfront payment option with standard 3-years term

These three options contradict the details provided earlier in the explanation, so these options are incorrect.

Reference:

https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf

Domain
Billing and Pricing

Question 56
A startup wants to migrate its data and applications from the on-premises data center to AWS Cloud. Which of the following options can be used by the startup to help with this migration? (Select two)

1] Utilize AWS Partner Network (APN) to build a custom solution for this infrastructure migration
2] Raise a support ticket with AWS Support for further assistance
3] Use AWS Trusted Advisor to automate the infrastructure migration
4] Leverage AWS Professional Services to accelerate the infrastructure migration
5] Consult moderators on AWS Developer Forums

Overall explanation
Correct options:

Leverage AWS Professional Services to accelerate the infrastructure migration

The AWS Professional Services organization is a global team of experts that can help you realize your desired business outcomes when using the AWS Cloud. AWS Professional Services consultants can supplement your team with specialized skills and experience that can help you achieve quick results. Therefore, leveraging AWS Professional Services can accelerate the infrastructure migration for the startup.

Utilize AWS Partner Network (APN) to build a custom solution for this infrastructure migration

The AWS Partner Network (APN) is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers. The startup can work with experts from APN to build a custom solution for this infrastructure migration.

Incorrect options:

Raise a support ticket with AWS Support for further assistance - AWS Support cannot help with complex infrastructure migration of this nature. Hence this option is incorrect.

Consult moderators on AWS Developer Forums - This is a made-up option and has been added as a distractor.

Use AWS Trusted Advisor to automate the infrastructure migration - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Trusted Advisor cannot automate the infrastructure migration.

References:

https://aws.amazon.com/partners/

https://aws.amazon.com/professional-services/

https://aws.amazon.com/solutions/implementations/aws-landing-zone/

Domain
Cloud Concepts

Question 57
Which AWS Support plan provides architectural guidance contextual to your specific use-cases?

1] AWS Developer Support

2] AWS Business Support

3] AWS Enterprise On-Ramp Support
4] AWS Enterprise Support

Overall explanation
Correct option:

AWS Business Support

You should use AWS Business Support if you have production workloads on AWS and want 24x7 phone, email and chat access to technical support and architectural guidance in the context of your specific use-cases. You get full access to AWS Trusted Advisor Best Practice Checks. You also get access to Infrastructure Event Management for an additional fee.

Incorrect options:

AWS Developer Support - You should use AWS Developer Support if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours as well as general architectural guidance as you build and test. This plan only supports general architectural guidance.

AWS Enterprise Support - AWS Enterprise Support provides customers with concierge-like service where the main focus is helping the customer achieve their outcomes and find success in the cloud. With Enterprise Support, you get 24x7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative review and guidance based on your applications, and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts. This plan supports architectural guidance contextual to your application.

AWS Enterprise On-Ramp Support - You should use the AWS Enterprise On-Ramp Support plan if you have production/business critical workloads in AWS and want 24x7 access to technical support and need expert guidance to grow and optimize in the Cloud. This plan supports architectural guidance contextual to your application (one per year).

Reference:

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

Domain
Billing and Pricing

Question 58
A Project Manager, working on AWS for the first time, is confused about how credits are used in AWS. There are two credits available in the manager's account. Credit one is for $100, expires July 2022, and can be used for either Amazon S3 or Amazon EC2. Credit two is for $50, expires December 2022, and can be used only for Amazon EC2. The manager's AWS account has incurred two charges: $1000 for Amazon EC2 and $500 for Amazon S3.

What will be the outcome on the overall bill once the credits are used? (Select two)

1] Only one credit can be used in one billing cycle and the customer has a choice to choose from the available ones

2] Credit one is applied, which expires in July, to the Amazon EC2 charge which leaves you with a $900 Amazon EC2 charge and a $500 Amazon S3 charge

3] Then, credit two is applied to $500 for Amazon S3 usage

4] Credit one is applied, which expires in July, to Amazon S3 usage which leaves you with a $1000 Amazon EC2 charge and a $400 Amazon S3 charge

5] Then, credit two is applied to the remaining $900 of Amazon EC2 usage

Overall explanation
Correct options:

Credit one is applied, which expires in July, to the Amazon EC2 charge which leaves you with a $900 Amazon EC2 charge and a $500 Amazon S3 charge

Then, credit two is applied to the remaining $900 of Amazon EC2 usage

Credits are applied in the following order:

Soonest expiring

Least number of applicable products

Oldest credit

For the given use case, credit one is applied, which expires in July, to the Amazon EC2 charge which leaves you with a $900 Amazon EC2 charge and a $500 Amazon S3 charge. Then, credit two is applied to the remaining $900 of Amazon EC2 usage. You need to pay $850 for Amazon EC2 and $500 for Amazon S3. All your credits are now exhausted.

Incorrect options:

Credit one is applied, which expires in July, to Amazon S3 usage which leaves you with a $1000 Amazon EC2 charge and a $400 Amazon S3 charge

Only one credit can be used in one billing cycle and the customer has a choice to choose from the available ones

Then, credit two is applied to $500 for Amazon S3 usage

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

Reference:

https://www.amazonaws.cn/en/support/faqs/

Domain
Billing and Pricing

Question 59

Which AWS services can be used to facilitate organizational change management, part of the Reliability pillar of AWS Well-Architected Framework? (Select three)

1] AWS Trusted Advisor
2] Amazon CloudWatch

3] AWS Config
4] AWS CloudTrail
5] Amazon Inspector
6] Amazon GuardDuty

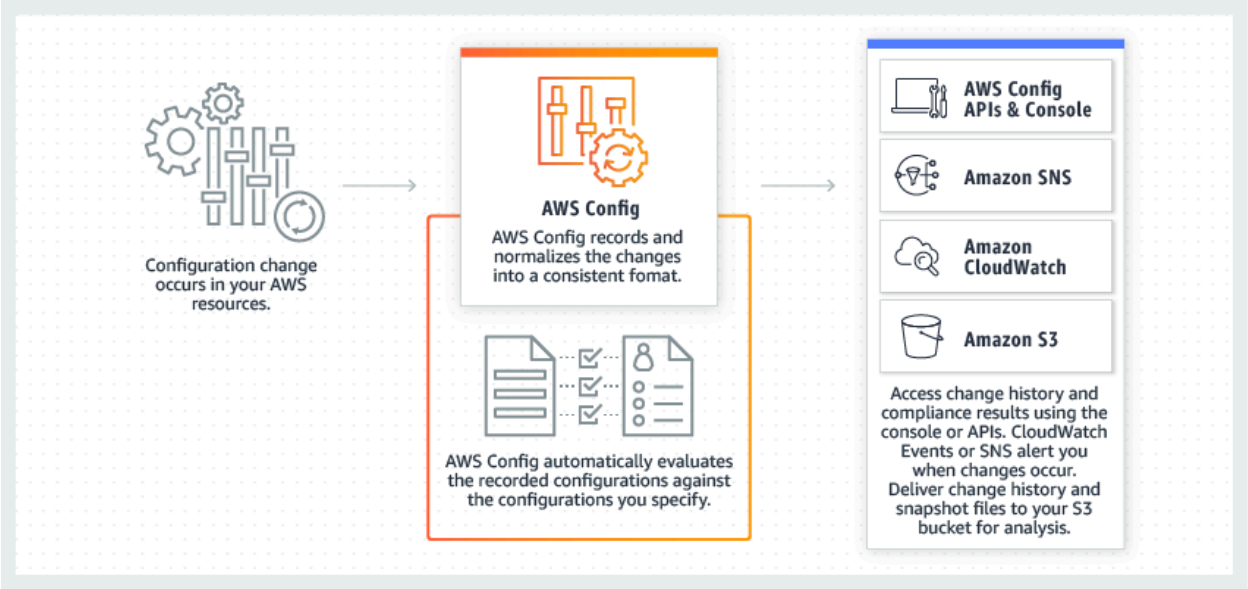
Overall explanation
Correct options:

There are three best practice areas for Reliability in the cloud - Foundations, Change Management, Failure Management. Being aware of how change affects a system (change management) allows you to plan proactively, and monitoring allows you to quickly identify trends that could lead to capacity issues or SLA breaches.

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.

How AWS Config Works:

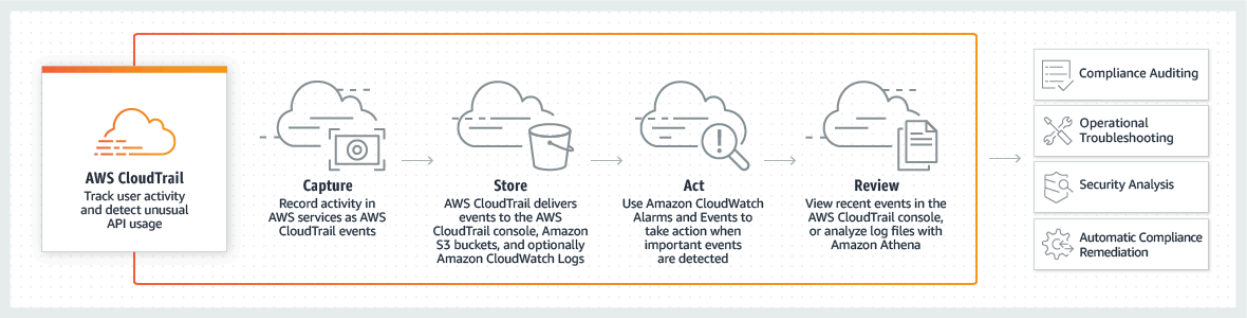


via - https://aws.amazon.com/config/

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.

How CloudTrail Works:



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

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

Incorrect options:

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 on cost optimization, security, fault tolerance, service limits, and performance improvement.

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.

Amazon GuardDuty - Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). This service is for AWS account level access, not for instance-level management like an EC2. GuardDuty cannot be used to check OS vulnerabilities.

References:

https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

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

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

Domain
Technology

Question 60

Which of the following entities applies patches to the underlying OS for Amazon Aurora?

1] The AWS Product Team automatically
2] The AWS customer by SSHing on the instances
3] The AWS Support after receiving a request from the customer
4] The AWS customer by using AWS Systems Manager

Overall explanation
Correct option:

The AWS Product Team automatically

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud. Amazon Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning,

database setup, patching, and backups. The AWS Product team is responsible for applying patches to the underlying OS for AWS Aurora.

Incorrect options:

The AWS customer by using AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks such as running commands, managing patches and configuring servers across AWS Cloud as well as on-premises infrastructure. You can only use AWS Systems Manager to apply patches to your EC2 instances or on-premises instances. You cannot use Systems Manager to apply patches to the underlying OS for AWS Aurora.

The AWS Support after receiving a request from the customer - AWS Support handles support tickets regarding AWS services. AWS Support is not responsible for applying patches to the underlying OS for AWS Aurora.

The AWS customer by SSHing on the instances - AWS customers are only responsible for patching their own EC2 instances.

Reference:

https://aws.amazon.com/rds/aurora/

Domain
Technology

Question 61
A company wants to identify the optimal AWS resource configuration for its workloads so that the company can reduce costs and increase workload performance. Which of the following services can be used to meet this requirement?

1] AWS Systems Manager
2] AWS Budgets
3] AWS Compute Optimizer
4] AWS Cost Explorer
5] Overall explanation

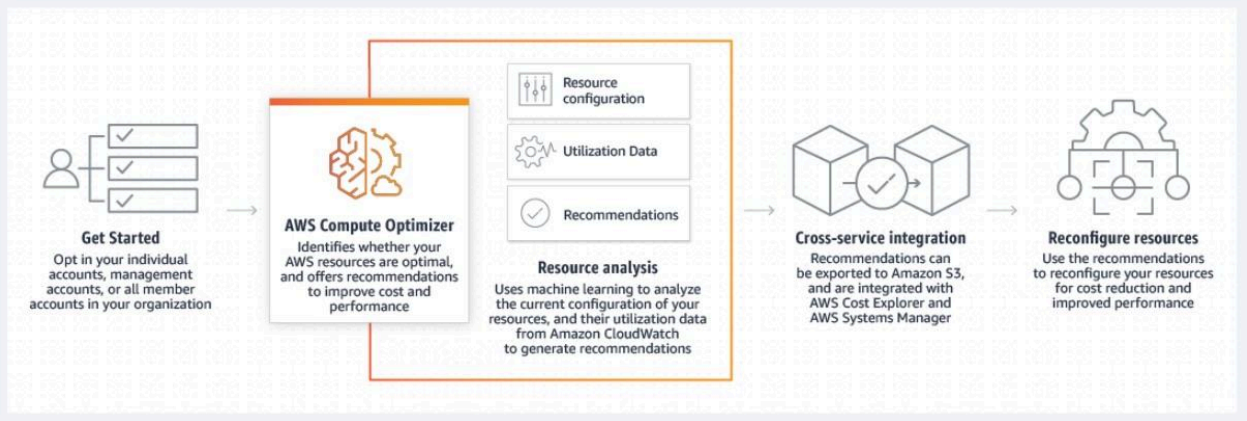
Correct option:

AWS Compute Optimizer

AWS Compute Optimizer recommends optimal AWS resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics. Over-provisioning resources can lead to unnecessary infrastructure costs, and under-provisioning resources can lead to poor application performance. Compute Optimizer helps you choose optimal configurations for three types of AWS resources: Amazon EC2 instances, Amazon EBS volumes, and AWS Lambda functions, based on your utilization data.

Compute Optimizer recommends up to 3 options from 140+ EC2 instance types, as well as a wide range of EBS volume and Lambda function configuration options, to right-size your workloads. Compute Optimizer also projects what the CPU utilization, memory utilization, and run time of your workload would have been on recommended AWS resource options. This helps you understand how your workload would have performed on the recommended options before implementing the recommendations.

How Compute Optimizer works:



via - https://aws.amazon.com/compute-optimizer/

Incorrect options:

AWS Systems Manager - AWS Systems Manager is the operations hub for AWS. Systems Manager provides a unified user interface so you can track and resolve operational issues across your AWS applications and resources from a central place.

With Systems Manager, you can automate operational tasks for Amazon EC2 instances or Amazon RDS instances. You can also group resources by application, view operational data for monitoring and troubleshooting, implement pre-approved change workflows, and audit operational changes for your groups of resources. Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easier to operate and manage your infrastructure at scale. Systems Manager cannot be used to identify the optimal resource configuration for workloads running on AWS.

AWS Budgets - AWS Budgets allows you to set custom budgets to track your cost and usage from the simplest to the most complex use cases. With AWS Budgets, you can choose to be alerted by email or SNS notification when actual or forecasted cost and usage exceed your budget threshold, or when your actual RI and Savings Plans' utilization or coverage drops below your desired threshold. With AWS Budget Actions, you can also configure specific actions to respond to cost and usage status in your accounts, so that if your cost or usage exceeds or is forecasted to exceed your threshold, actions can be executed automatically or with your approval to reduce unintentional over-spending.

AWS Cost Explorer - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. Cost Explorer Resource Rightsizing Recommendations and Compute Optimizer use the same recommendation engine. The Compute Optimizer recommendation engine delivers recommendations to help customers identify optimal EC2 instance types for their workloads. The Cost Explorer console and API surface a subset of these recommendations that may lead to cost savings, and augments them with customer-specific cost and savings information (e.g. billing information, available credits, RI, and Savings Plans) to help Cost Management owners quickly identify savings opportunities through infrastructure rightsizing. Compute Optimizer console and its API delivers all recommendations regardless of the cost implications.

Reference:

https://aws.amazon.com/compute-optimizer/

Domain
Technology

Question 62
Which of the following is CORRECT regarding removing an AWS account from AWS Organizations?
1] The AWS account must not have any Service Control Policies (SCPs) attached to it. Only then it can be removed from AWS organizations
2] The AWS account can be removed from AWS Systems Manager
3] Raise a support ticket with AWS Support to remove the account
4] The AWS account must be able to operate as a standalone account. Only then it can be removed from AWS organizations

Overall explanation
Correct option:

The AWS account must be able to operate as a standalone account. Only then it can be removed from AWS organizations

You can remove an account from your organization only if the account has the information that is required for it to operate as a standalone account. For each account that you want to make standalone, you must accept the AWS Customer Agreement, choose a support plan, provide and verify the required contact information, and provide a current payment method. AWS uses the payment method to charge for any billable (not AWS Free Tier) AWS activity that occurs while the account isn't attached to an organization.

Incorrect options:

Raise a support ticket with AWS Support to remove the account - AWS Support does not need to help you in removing an AWS account from AWS Organizations.

The AWS account can be removed from AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks such as running

commands, managing patches, and configuring servers across AWS Cloud as well as on-premises infrastructure. Systems Manager cannot be used to remove an AWS account from AWS Organizations.

The AWS account must not have any Service Control Policies (SCPs) attached to it. Only then it can be removed from AWS organizations - This is not a pre-requisite to remove the AWS account. The principals in the AWS account are no longer affected by any service control policies (SCPs) that were defined in the organization. This means that restrictions imposed by those SCPs are gone, and the users and roles in the account might have more permissions than they had before.

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_remove.html

Domain
Cloud Concepts

Question 63

Which of the following AWS services has encryption enabled by default?
1] AWS CloudTrail Logs
2] Amazon Elastic File System (Amazon EFS)
3] Amazon Relational Database Service (Amazon RDS)
4] Amazon Elastic Block Store (Amazon EBS)

Overall explanation
Correct option:

AWS CloudTrail Logs

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. AWS CloudTrail can be used to record AWS API calls and other activity for your AWS account and save the recorded information to log files in an Amazon Simple Storage Service (Amazon S3) bucket that you choose. By

default, the log files delivered by CloudTrail to your S3 bucket are encrypted using server-side encryption with Amazon S3 managed keys (SSE-S3).

Incorrect options:

Amazon Elastic File System (Amazon EFS) - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. This is an optional feature and has to be enabled by user if needed.

Amazon Elastic Block Store (Amazon EBS) - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) instances for both throughput and transaction-intensive workloads at any scale. Encryption (at rest and during transit) is an optional feature for EBS and has to be enabled by the user.

Amazon Relational Database Service (Amazon RDS) - Amazon Relational Database Service (Amazon RDS) can encrypt your Amazon RDS DB instances. Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, read replicas, and snapshots. Encryption for RDS is an additional feature and the user needs to enable it.

Reference:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html

Domain
Security and Compliance

Question 64

Which of the following AWS services should be used to automatically distribute incoming traffic across multiple targets?

1] AWS Auto Scaling
2] AWS Elastic Beanstalk

3] AWS Elastic Load Balancing (ELB)
4] Amazon OpenSearch Service

Overall explanation
Correct option:

AWS Elastic Load Balancing (ELB)

Elastic Load Balancing (ELB) is used to automatically distribute your incoming application traffic across all the EC2 instances that you are running. You can use Elastic Load Balancing to manage incoming requests by optimally routing traffic so that no one instance is overwhelmed. Your load balancer acts as a single point of contact for all incoming web traffic to your application. When an instance is added, it needs to register with the load balancer or no traffic is routed to it. When an instance is removed, it must deregister from the load balancer or traffic continues to be routed to it.

Incorrect options:

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed in a variety of programming languages. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. You cannot use Beanstalk to distribute incoming traffic across multiple targets.

Amazon OpenSearch Service - Amazon OpenSearch Service makes it easy for you to perform interactive log analytics, real-time application monitoring, website search, and more. OpenSearch is an open source, distributed search and analytics suite derived from Elasticsearch.

AWS Auto Scaling - AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it’s easy to setup application scaling for multiple resources across multiple services in minutes. This is a scaling service that helps you spin up resources as and when you need them and scale down when the high demand

reduces. Auto Scaling can be used with Elastic Load Balacing to build high performance applications.

Reference:

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

Domain
Technology

Question 65
A company uses reserved EC2 instances across multiple units with each unit having its own AWS account. However, some of the units under-utilize their reserved instances while other units need more reserved instances. As a Cloud Practitioner, which of the following would you recommend as the most cost-optimal solution?

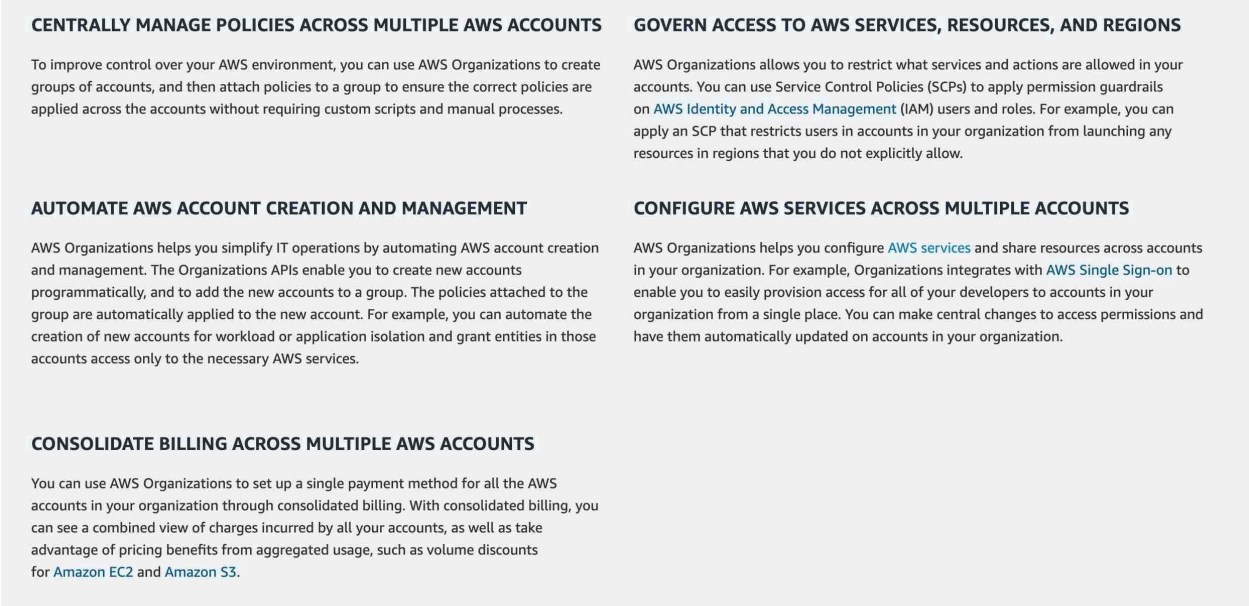
1] Use AWS Systems Manager to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units
2] Use AWS Cost Explorer to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units
3] Use AWS Organizations to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units
4] Use AWS Trusted Advisor to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units

Overall explanation
Correct option:

Use AWS Organizations to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units

AWS Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts. Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance. You can also simplify billing by setting up a single payment method for all of your AWS accounts. AWS Organizations is available to all AWS customers at no additional charge.

Key Features of AWS Organizations:

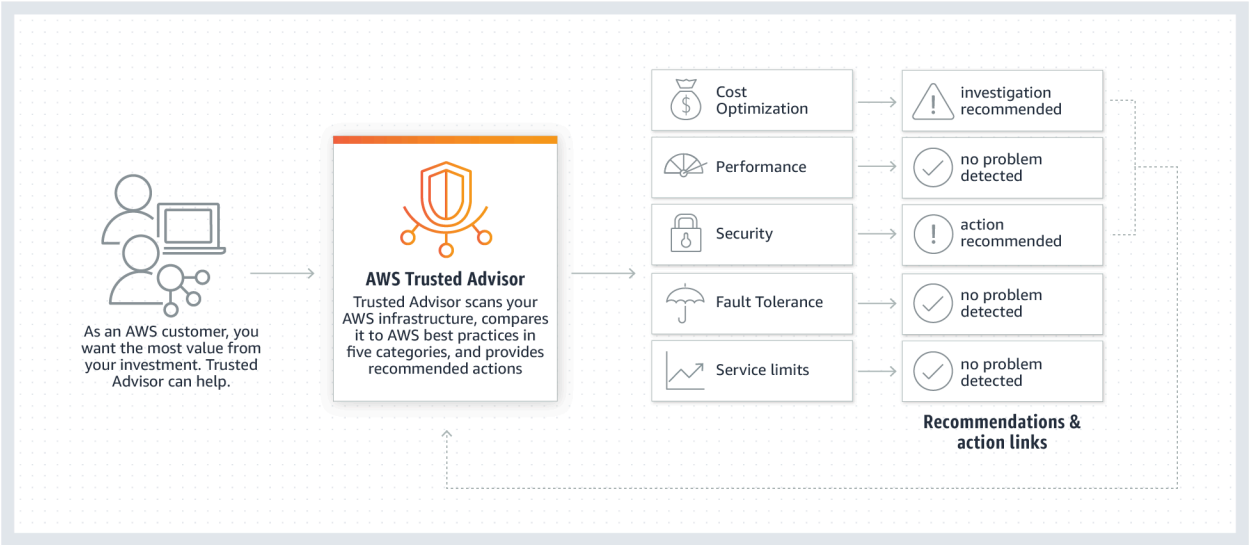


via - https://aws.amazon.com/organizations/

Incorrect options:

Use AWS Trusted Advisor to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. You cannot use Trusted Advisor to share the reserved EC2 instances amongst multiple AWS accounts.

How Trusted Advisor Works:

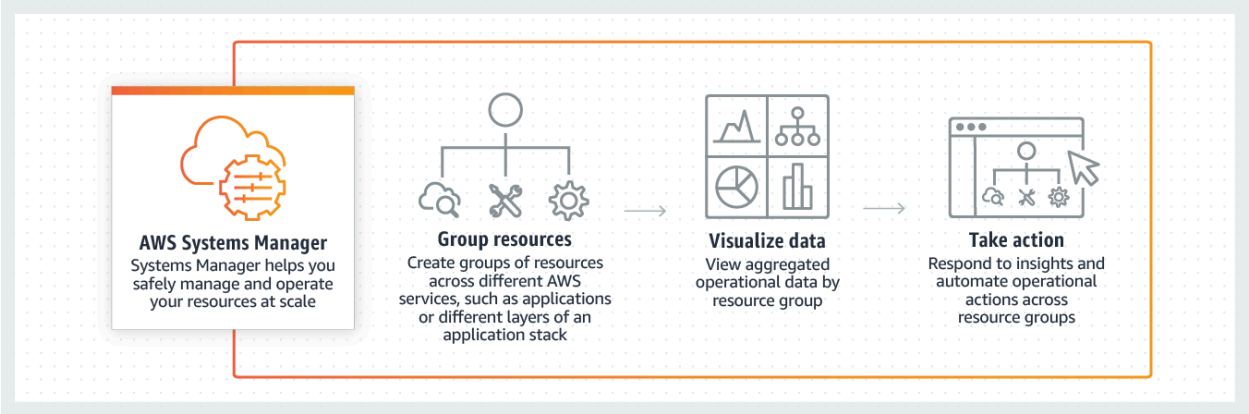


via - https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

Use AWS Cost Explorer to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units - AWS Cost Explorer lets you explore your AWS costs and usage at both a high level and at a detailed level of analysis, and empowering you to dive deeper using several filtering dimensions (e.g., AWS Service, Region, Linked Account). You cannot use Cost Explorer to share the reserved EC2 instances amongst multiple AWS accounts.

Use AWS Systems Manager to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units - Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. You cannot use Systems Manager to share the reserved EC2 instances amongst multiple AWS accounts.

How AWS Systems Manager Works:



via - https://aws.amazon.com/systems-manager/

References:

https://aws.amazon.com/organizations/

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

https://aws.amazon.com/systems-manager/