Question 1:
Which pillar of the AWS Well-Architected Framework recommends monitoring your application's performance?

Explanation
Correct option:

Performance Efficiency

The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement.

The AWS Well-Architected Framework is based on five pillars — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.

The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

After you have implemented your architecture you will need to monitor its performance so that you can remediate any issues before your customers are aware. Monitoring metrics should be used to raise alarms when thresholds are breached.

Incorrect options:

Reliability - The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross-project requirements, recovery planning, and how we handle change.

Operational Excellence - The Operational Excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events.

Security - The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

Reference:

https://wa.aws.amazon.com/wat.pillar.performance.en.html

Question 2:

Which AWS Route 53 routing policy would you use when you want to route your traffic in an active-passive configuration?

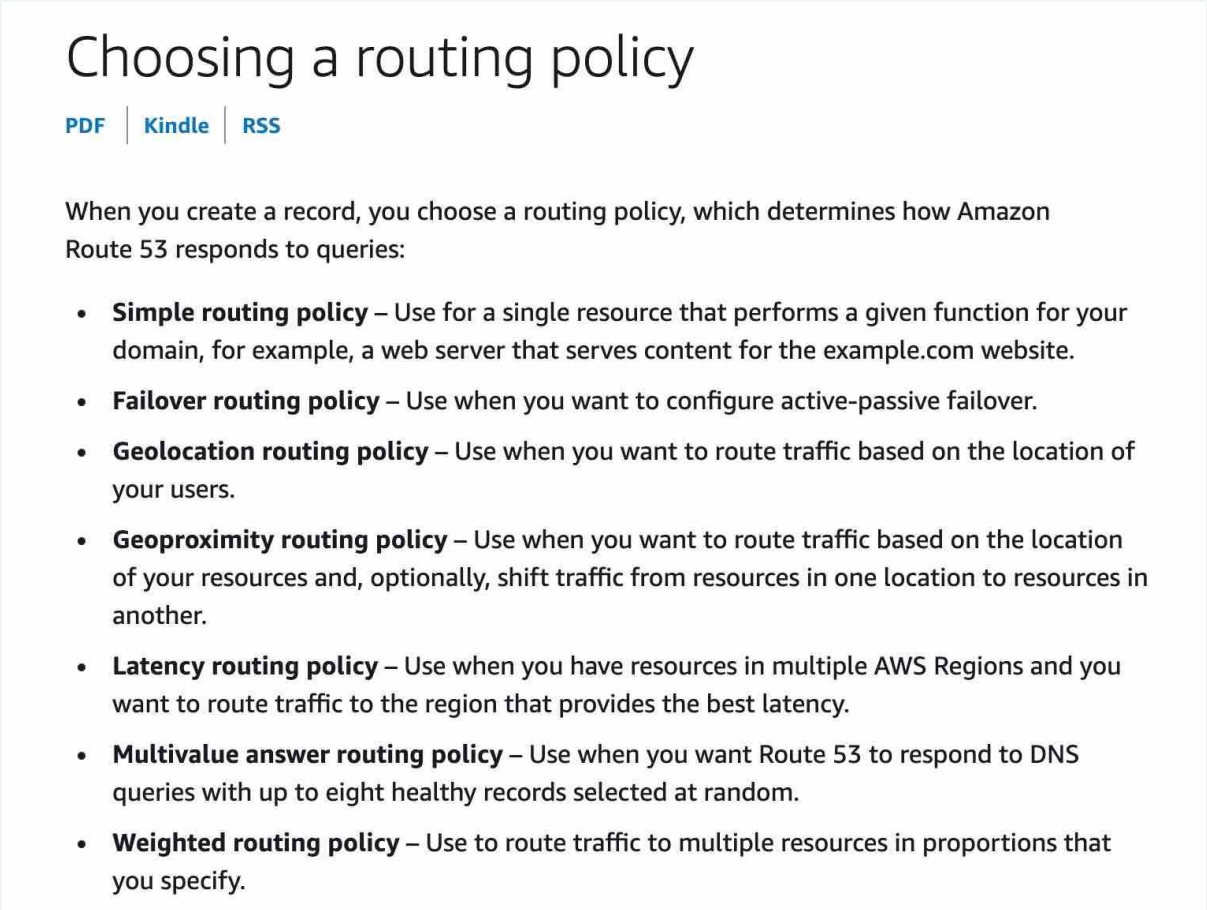
Explanation
Correct option:

Failover routing policy

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.

Failover routing policy is used when you want to configure active-passive failover. Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. The primary and secondary records can route traffic to anything from an Amazon S3 bucket that is configured as a website to a complex tree of records.

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:

Simple routing policy - Simple routing lets you configure standard DNS records, with no special Route 53 routing such as weighted or latency. With simple routing, you typically route traffic to a single resource, for example, to a web server for your website.

Weighted routing policy - This routing policy is used to route traffic to multiple resources in proportions that you specify.

Latency routing policy - 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

Question 3:
Which budget types can be created under AWS Budgets (Select three)?
Explanation
Correct options:

AWS Budgets enable you to plan your service usage, service costs, and instance reservations. AWS Budgets information is updated up to three times a day. Updates typically occur between 8 to 12 hours after the previous update. Budgets track your unblended costs, subscriptions, refunds, and RIs. There are four different budget types you can create under AWS Budgets - Cost budget, Usage budget, Reservation budget and Savings Plans budget.

Cost budget - Helps you plan how much you want to spend on a service.

Usage budget - Helps you plan how much you want to use one or more services.

Reservation budget - This helps you track the usage of your Reserved Instances (RI). Two ways of doing it - RI utilization budgets (This lets you see if your RIs are unused or under-utilized), RI coverage budgets (This lets you see how much of your instance usage is covered by a reservation).

Incorrect options:

Resource budget - This is a made-up option and has been added as a distractor

Software budget - This is a made-up option and has been added as a distractor

Hardware budget - This is a made-up option and has been added as a distractor

Reference:

This is a made-up option and has been added as a distractor

Question 4:
An IT company would like to move its IT infrastructure from an AWS Region in the US to another AWS Region in Europe. Which of the following represents the correct solution for this use-case?

- The company should raise a ticket with AWS Support for this infrastructure migration
- The company should just start creating new resources in the destination AWS Region and then migrate the relevant data and applications into this new AWS Region **(Correct)**
- The company should use Database Migration Service to move the resources from source AWS Region to destination AWS Region
- The company should use CloudFormation to move the resources from source AWS Region to destination AWS Region

Explanation
Correct option:

The company should just start creating new resources in the destination AWS Region and then migrate the relevant data and applications into this new AWS Region - The company needs to create resources in the new AWS Region and then move the relevant data and applications into the new AWS Region. There is no off-the-shelf solution or service that the company can use to facilitate this transition.

Incorrect options:

The company should use CloudFormation to move the resources from source AWS Region to destination AWS Region - 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 cannot help with IT infrastructure migration.

The company should use Database Migration Service to move the resources from source AWS Region to destination AWS Region - AWS Database Migration Service 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 can migrate your data to and from the most widely used commercial and open-source databases. Database Migration Service cannot help with the entire IT infrastructure migration.

The company should raise a ticket with AWS Support for this infrastructure migration - This option has been added as a distractor. AWS Support cannot help with IT infrastructure migration.

Question 5:
A financial services enterprise plans to enable Multi-Factor Authentication (MFA) for its employees. For ease of travel, they prefer not to use any physical devices to implement MFA. Which of the below options is best suited for this use case?

-

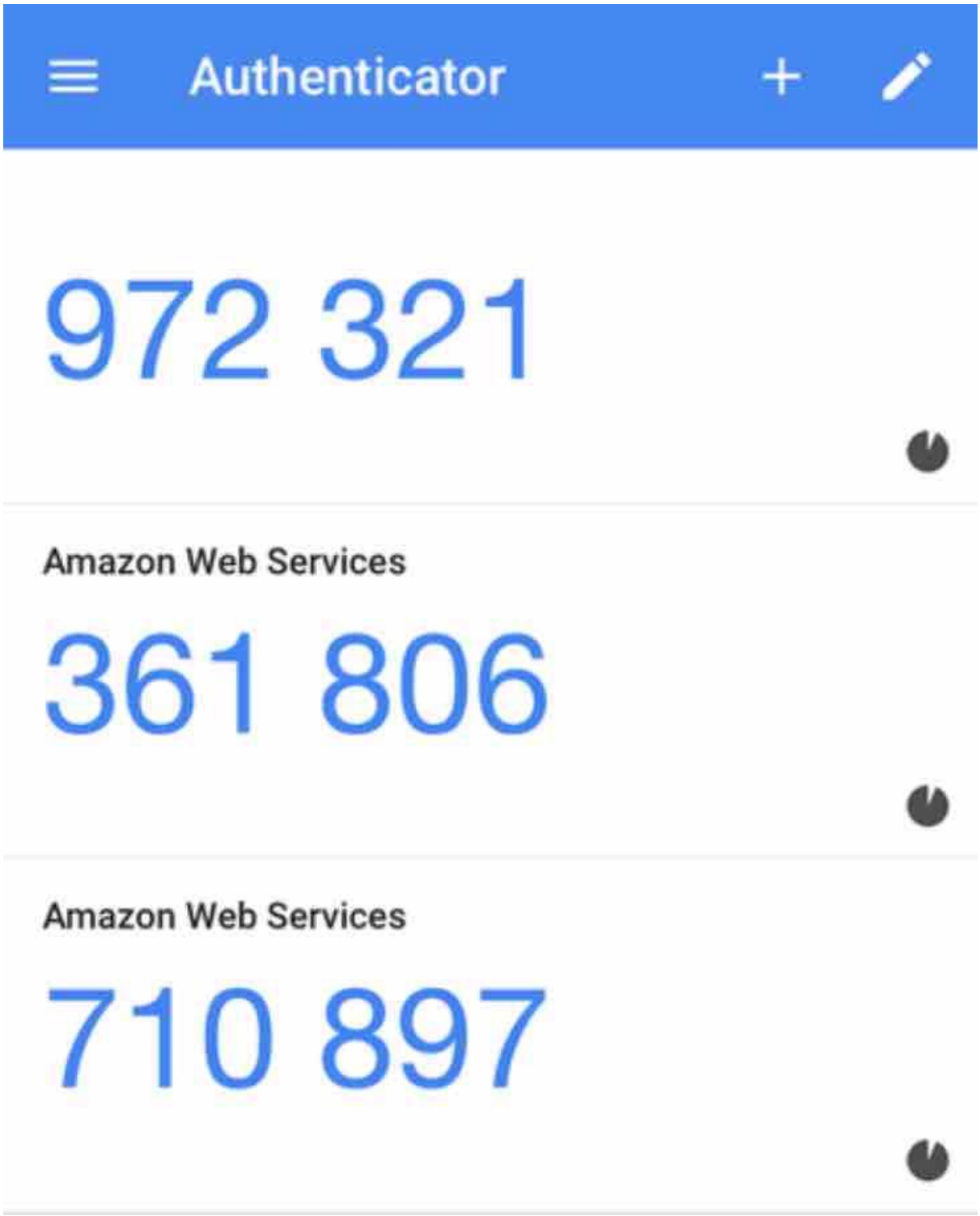
Explanation

Correct option:

Virtual MFA device

A software app that runs on a phone or other device and emulates a physical device. The device generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each virtual MFA device assigned to a user must be unique. A user cannot type a code from another user's virtual MFA device to authenticate.

Google Authenticator is an example of a Virtual MFA device:



Incorrect options:

U2F security key - A device that you plug into a USB port on your computer. U2F is an open authentication standard hosted by the FIDO Alliance. When you enable a U2F security key, you sign in by entering your credentials and then tapping the device instead of manually entering a code.

Hardware MFA device - A hardware device that generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each MFA device assigned to a user must be unique. A user cannot type a code from another user's device to be authenticated.

Soft Token MFA device - This is a made-up option and has been added as a distractor.

Reference:

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

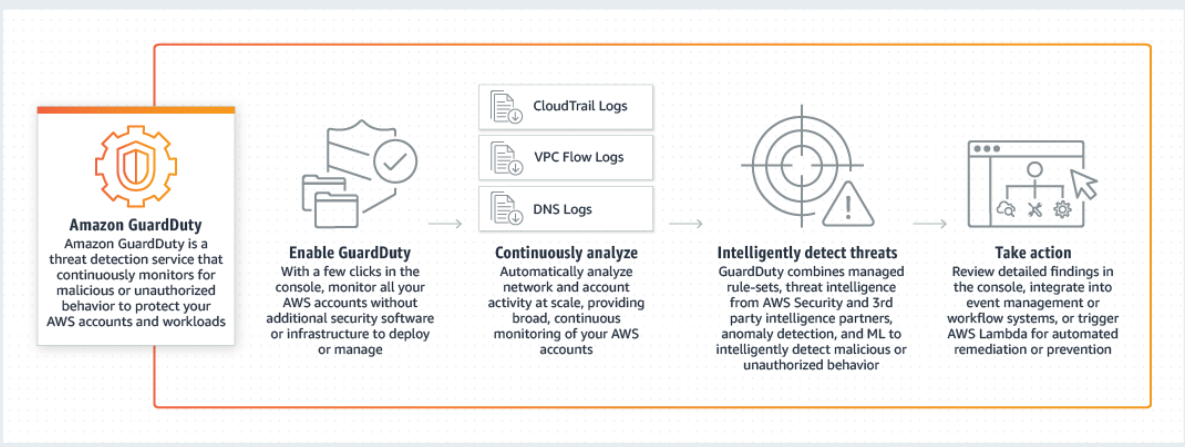
Question 6: Correct
Which AWS service protects your AWS account by monitoring malicious activity and detecting threats?

Explanation
Correct option:

GuardDuty

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). Security findings are retained and made available through the Amazon GuardDuty console and APIs for 90-days. After 90-days, the findings are discarded. To retain findings for longer than 90-days, you can enable AWS CloudWatch Events to automatically push findings to an Amazon S3 bucket in your account or another data store for long-term retention.

How GuardDuty Works:



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

Incorrect options:

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. Think account-specific activity and audit; think CloudTrail. CloudTrail cannot detect threats to your AWS account.

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 your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot detect threats to your AWS account.

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. Trusted Advisor cannot detect threats to your AWS account.

Reference:

https://aws.amazon.com/guardduty

Question 7: **Correct**
An AWS hardware failure has impacted one of your EBS volumes. Which AWS service will alert you of the affected resources and provide a remedial action?
Explanation
Correct option:

AWS Personal Health Dashboard

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view of the performance and availability of the AWS services underlying your AWS resources. The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues. For example, in the event of an AWS hardware failure impacting one of your EBS volumes, you will get an alert that includes a list of your affected resources, a recommendation to restore your volume, and links to the steps to help you restore it from a snapshot.

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).

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.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides 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 on a regular basis help keep your solutions provisioned optimally.

Reference:

https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/

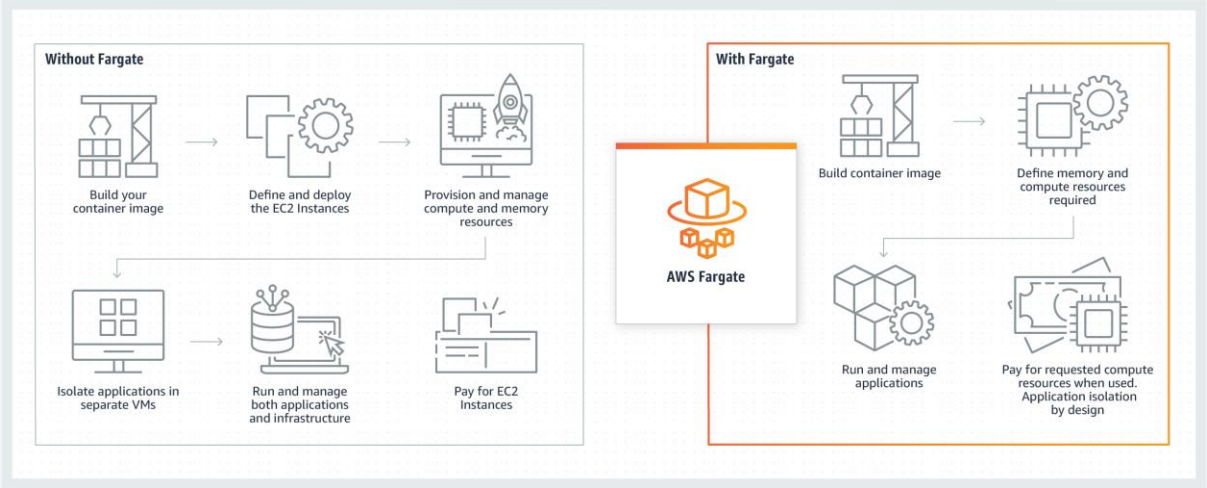
Question 8: **Correct**
A startup runs its proprietary application on docker containers. As a Cloud Practitioner, which AWS service would you recommend so that the startup can run containers and still have access to the underlying servers?
Explanation
Correct option:

Amazon Elastic Container Service (Amazon ECS) - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster. This is not a fully managed service and you can manage the underlying servers yourself.

Incorrect options:

AWS Fargate - AWS Fargate is a serverless compute engine for containers. It works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. With Fargate, you do not have access to the underlying servers, so this option is incorrect.

How Fargate
Works:



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

AWS Lambda - AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. Lambda does not support running container applications.

Amazon Elastic Container Registry (ECR) - Amazon Elastic Container Registry (ECR) can be used to store, manage, and deploy Docker container images. Amazon ECR eliminates the need to operate your container repositories. ECR does not support running container applications.

Reference:

https://aws.amazon.com/fargate/

Question 9: Correct
A cyber-security agency uses AWS Cloud and wants to carry out security assessments on their own AWS infrastructure without any prior approval from AWS. Which of the following describes/facilitates this practice?

Explanation
Correct option:

Penetration Testing

AWS customers can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for few common AWS services. Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves.

Incorrect options:

Network Stress Testing - AWS considers "network stress test" to be when a test sends a large volume of legitimate or test traffic to a specific intended target application. The endpoint and infrastructure are expected to be able to handle this traffic.

Amazon Inspector - Amazon Inspector is an automated, security assessment service that helps you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.

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.

Reference:

https://aws.amazon.com/security/penetration-testing/

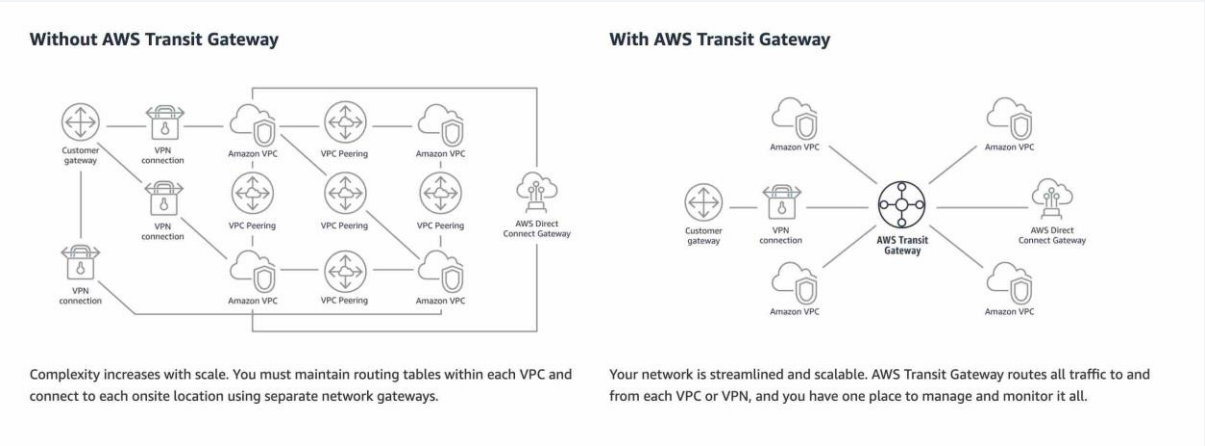
Question 10: **Correct**
An organization maintains separate VPCs for each of its departments. With expanding business, the organization now wants to connect all VPCs for better departmental collaboration. Which AWS service will help the organization tackle the issue effectively?

Explanation
Correct option:

AWS Transit Gateway

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. As you expand globally, inter-Region peering connects AWS Transit Gateways using the AWS global network. Your data is automatically encrypted and never travels over the public internet.

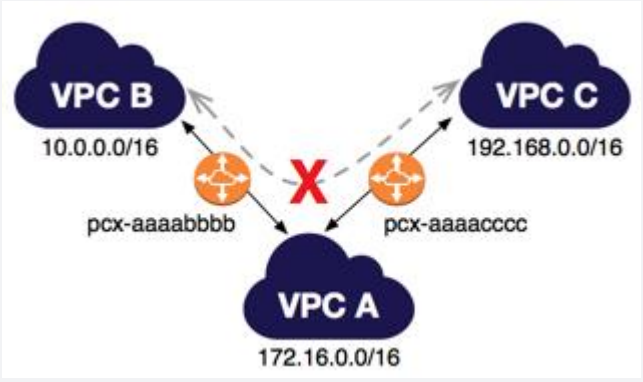
How Transit Gateway can simplify your network:



via - https://aws.amazon.com/transit-gateway/

Incorrect options:

VPC Peering - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. VPC peering is not transitive, a separate VPC peering connection has to be made between two VPCs that need to talk to each other. With growing VPCs, this gets difficult to manage.

Transitive VPC Peering is not allowed: 

via - https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html

AWS Direct Connect - AWS Direct Connect creates a dedicated private connection from a remote network to your VPC. This is a private connection and does not use the public internet. Takes at least a month to establish this connection. Direct Connect cannot be used to interconnect VPCs.

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. Site to Site VPN cannot be used to interconnect VPCs.

Reference:

https://aws.amazon.com/transit-gateway/

Question 11:
Data encryption is automatically enabled for which of the following AWS services? (Select two)?

Explanation
Correct option:
Cloud trails also auto enable encryption ***imp

Amazon S3 Glacier - Amazon S3 Glacier (S3 Glacier), is a storage service optimized for infrequently used data, or "cold data. Data at rest stored in S3 Glacier is automatically server-side encrypted using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways - File, Volume and Tape Gateways).

Incorrect options:

Amazon EBS volumes - Amazon EBS volumes are not encrypted, by default. You can configure your AWS account to enforce the encryption of the new EBS volumes and snapshot copies that you create.

Amazon Redshift - Encryption is an optional setting in Amazon Redshift. When you enable encryption for a cluster, the data-blocks and system metadata are encrypted for the cluster and its snapshots.

Amazon EFS drives - Encryption is not a default setting, but an optional configuration for EFS drives. Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest.

References:

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

https://docs.aws.amazon.com/amazonglacier/latest/dev/DataEncryption.html

Question 12:
Which AWS service can be used for online analytical processing?

Explanation
Correct option:

Amazon Redshift

Amazon Redshift is a fast, fully managed cloud data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It allows you to run complex analytic queries against terabytes to petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution.

Incorrect options:

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

Customers use Amazon RDS databases primarily for online-transaction processing (OLTP) workload while Redshift is used primarily for reporting and analytics.

Amazon DynamoDB - Amazon DynamoDB is a NoSQL database that supports key-value and document data models and enables developers to build modern, serverless applications that can start small and scale globally to support petabytes of data and tens of millions of read and write requests per second. DynamoDB supports both key-value and document data models. This enables DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases. DynamoDB cannot be used for online analytical processing.

Amazon ElastiCache - Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-Source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for real-time use cases like Caching, Session Stores, Gaming, Geospatial Services, Real-Time Analytics, and Queuing. ElastiCache cannot be used for online analytical processing.

Reference:

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

Question 13:
Which feature of AWS Cloud offers the ability to innovate faster and rapidly develop, test and launch software applications?

Explanation
Correct option:

Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS).

Agility - Agility refers to the ability of the cloud to give you easy access to a broad range of technologies so that you can innovate faster and build nearly anything that you can imagine. You can quickly spin up resources as you need them – from infrastructure services, such as compute, storage, and databases, to Internet of Things, machine learning, data lakes and analytics, and much more.

Incorrect options:

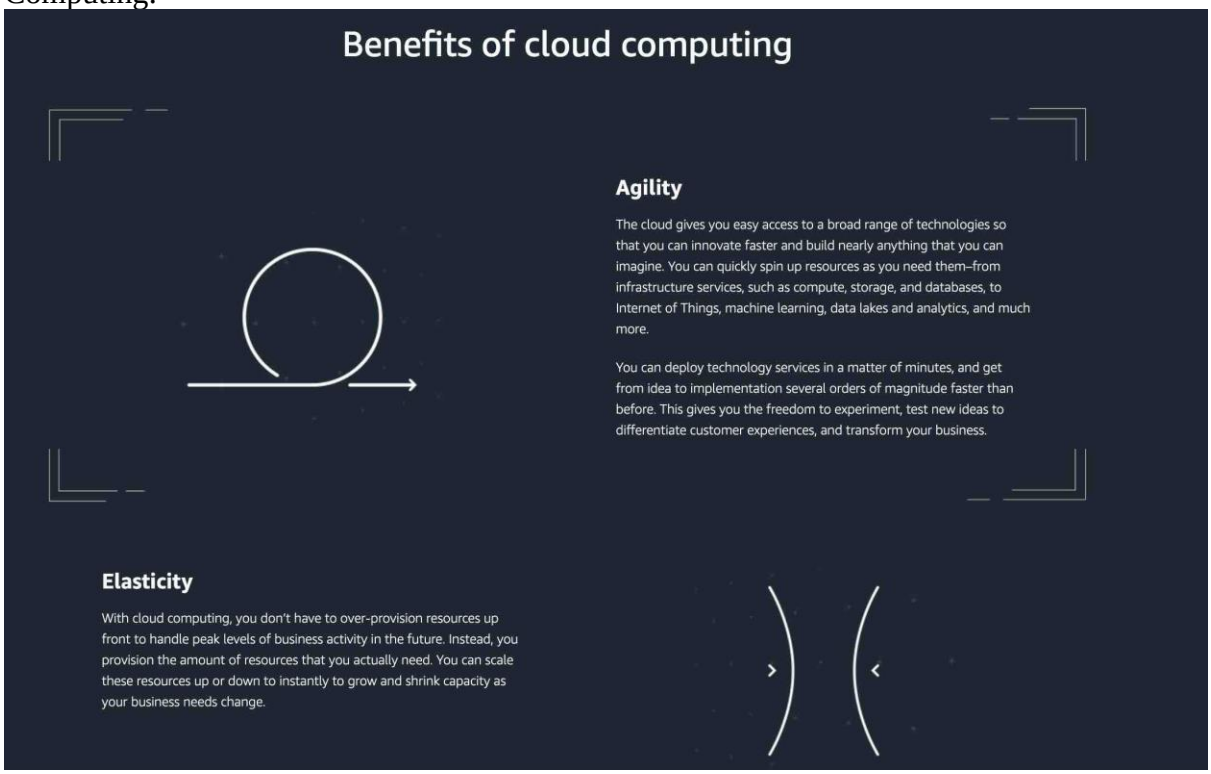
Elasticity - With cloud computing elasticity, you don't have to over-provision resources upfront to handle peak levels of business activity in the future. Instead, you provision the number of resources that you actually need. You can scale these resources up or down instantly to grow and shrink capacity as your business needs change.

Cost savings - The cloud allows you to trade capital expenses (such as data centers and physical servers) for variable expenses, and only pay for IT as you consume it. Plus, the variable expenses are much lower than what you would pay to do it yourself because of the economies of scale.

Ability to deploy globally in minutes - With the cloud, you can expand to new geographic regions and deploy globally in minutes. For example, AWS has infrastructure all over the world, so you can deploy your application in multiple physical locations with just a few clicks. Putting applications in closer proximity to end users reduces latency and improves their experience.

Exam Alert:

Please review the benefits of Cloud Computing:



via - https://aws.amazon.com/what-is-cloud-computing/

Reference:

https://aws.amazon.com/what-is-cloud-computing/

Question 14:

Which of the following statements is correct regarding the AWS Elastic File System (EFS) storage service?

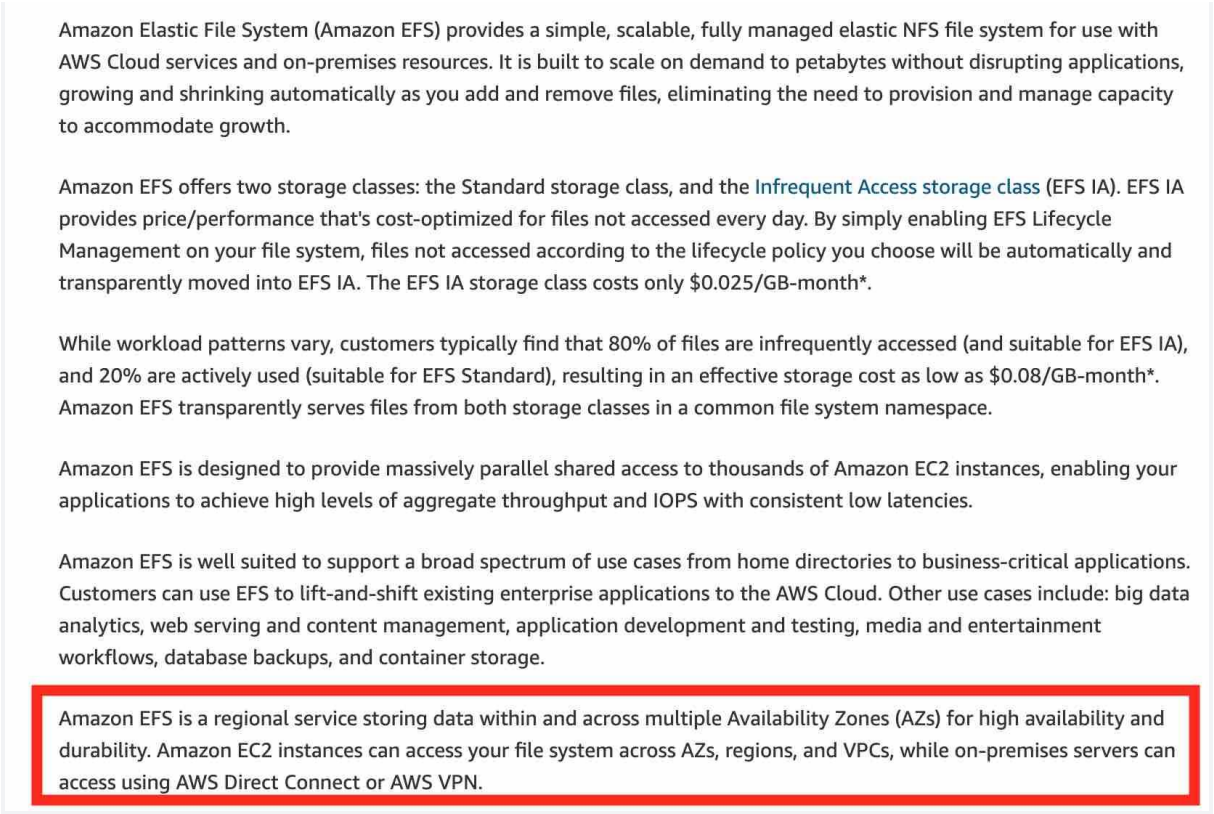
- EC2 instances can access files on an EFS file system across many Availability Zones, regions and VPCs **(Correct)**
- EC2 instances can access files on an EFS file system across many Availability Zones and VPCs
- EC2 instances can access files on an EFS file system across many Availability Zones
- EC2 instances can access files on an EFS file system only in one Availability Zone

Explanation
Correct option:

EC2 instances can access files on an EFS file system across many Availability Zones, regions and VPCs

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

Amazon EFS
Overview:



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

Incorrect options:

EC2 instances can access files on an EFS file system only in one Availability Zone

EC2 instances can access files on an EFS file system across many Availability Zones

EC2 instances can access files on an EFS file system across many Availability Zones and VPCs

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

Reference:

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

Question 15: Correct
Which of the following are correct statements regarding the AWS Shared Responsibility Model? (Select two)

- ☑ AWS is responsible for Security "of" the Cloud
  (Correct)
- ☑ For abstracted services like Amazon S3, AWS operates the infrastructure layer, the operating system, and platforms
  (Correct)

- For a service like Amazon EC2, that falls under Infrastructure as a Service, AWS is responsible for maintaining guest operating system
- AWS is responsible for training AWS and customer employees on AWS products and services
- Configuration Management is the responsibility of the customer

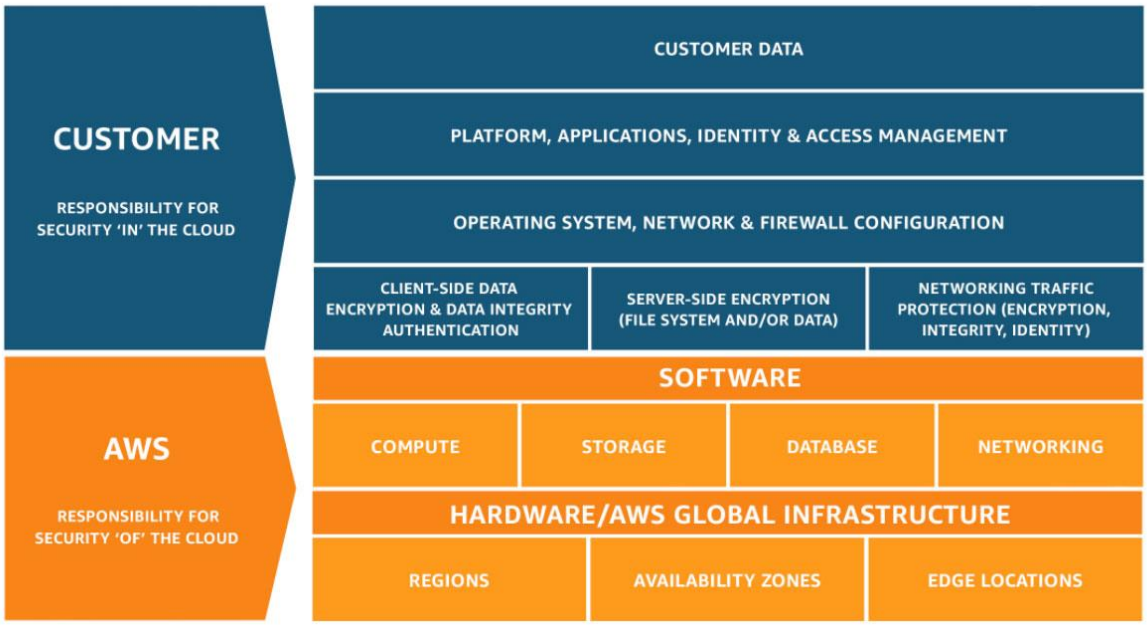
Explanation
Correct options:

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.

AWS is responsible for Security "of" the Cloud - 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.

"For abstracted services like Amazon S3, AWS operates the infrastructure layer, the operating system, and platforms" - 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:

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

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

AWS is responsible for training AWS and customer employees on AWS products and services - Awareness & Training is also a shared responsibility. AWS trains AWS employees, but a customer must train their own employees.

Reference:

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

Question 16: Correct
Amazon CloudWatch billing metric data is stored in which AWS Region?

Explanation
Correct option:

US East (N. Virginia) - us-east-1

You can monitor your estimated AWS charges by using Amazon CloudWatch. Billing metric data is stored in the US East (N. Virginia) Region and represents worldwide charges. This data includes the estimated charges for every service in AWS that you use, in addition to the estimated overall total of your AWS charges.

Incorrect options:

In the AWS Region where the AWS account is created

In the AWS Region where the AWS resource is provisioned

US West (N. California) - us-west-1

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

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charges_with_cloudwatch.html

Question 17: Correct
Which of the following statements are CORRECT about the AWS Auto Scaling group? (Select two)

- ☑

Explanation
Correct option:

Auto Scaling group scales out and adds more number of EC2 instances to match an increase in demand

Auto Scaling group scales in and reduces the number of EC2 instances to match a decrease in demand

AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas.

You can use scaling policies to increase or decrease the number of instances in your group dynamically to meet changing conditions. When the scaling policy is in effect, the Auto Scaling group adjusts the desired capacity of the group, between the minimum and maximum capacity values that you specify, and launches or terminates the instances as needed. You can also scale on a schedule.

Incorrect options:

Auto Scaling group scales down and reduces the number of EC2 instances to match a decrease in demand - A scale down refers to a downgrade to a less powerful EC2 instance. Therefore this option is incorrect.

Auto Scaling group scales down and downgrades to a less powerful EC2 instance to match a decrease in demand

Auto Scaling group scales up and upgrades to a more powerful EC2 instance to match an increase in demand

An Auto Scaling group does not scale up or scale down, so these two options are incorrect.

Reference:

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

Question 18: Correct
Compared to the On-demand prices, what is the highest possible discount offered for reserved instances?

- ◉
  72
- ○

50

40

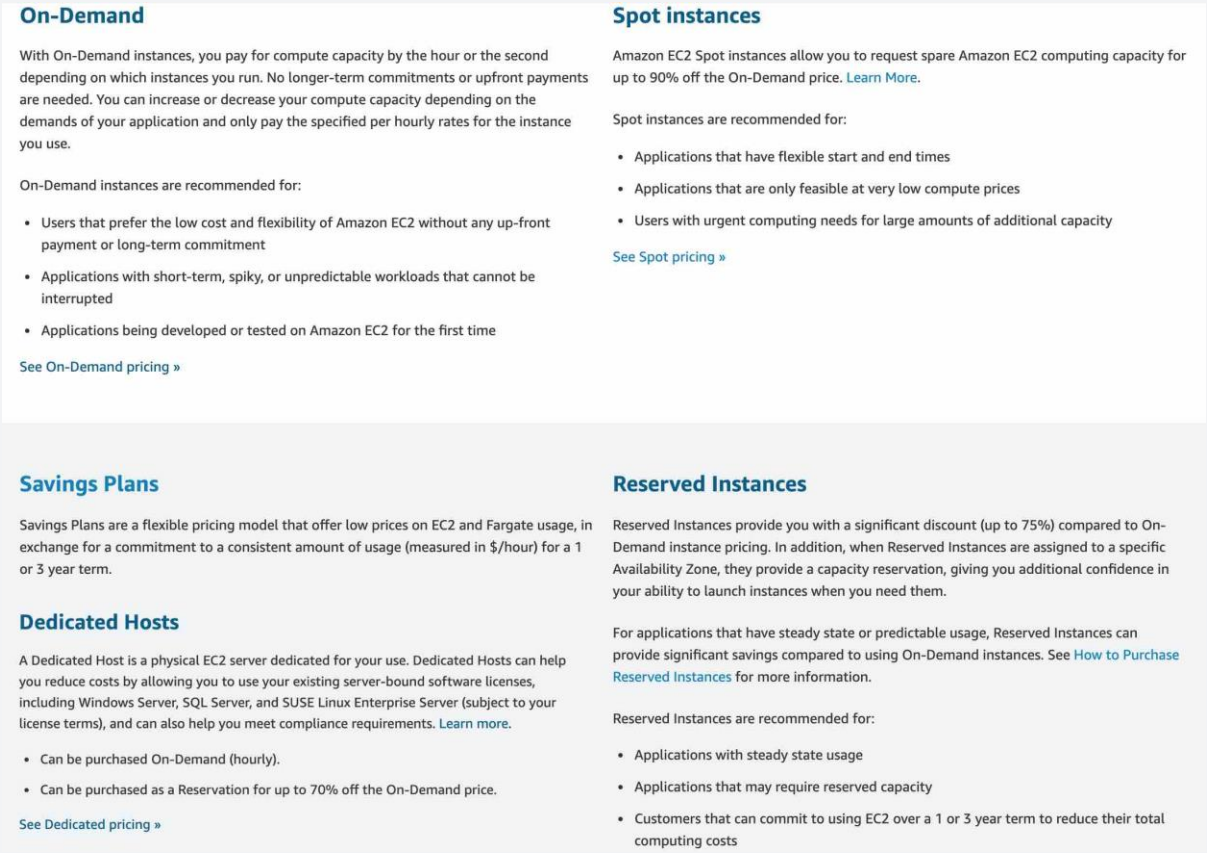
90

Explanation
Correct option:

72

Reserved Instances provide you with significant savings (up to 72%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount.

EC2 Pricing Options
Overview:



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

Incorrect options:

90

50

40

Reference:

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

Question 19: **Correct**
Which of the following is a part of the AWS Global Infrastructure?

- **Explanation**

Correct option:

Region

AWS Region is a physical location around the world where AWS builds its data centers. Each group of logical data centers is called an Availability Zone (AZ). Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area.

Please see this illustration for AWS regions in the
US:

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

Incorrect options:

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

Virtual Private Network (VPN) - AWS Virtual Private Network (AWS VPN) lets you establish a secure and private encrypted tunnel from your on-premises network to the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN.

Subnets - A subnet is a range of IP addresses within your VPC. A subnet spans only one Availability Zone in the Region.

These three options are not a part of the AWS Global Infrastructure.

Reference:

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

Question 20: **Correct**
A financial services company must meet compliance requirements that mandate storing multiple copies of data in geographically distant locations. As the company uses S3 as its main storage service, which of the following represents the MOST resource-efficient solution for this use-case?

Explanation
Correct option:

Use Cross-Region replication (CRR) to replicate data between distant AWS Regions

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

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region.

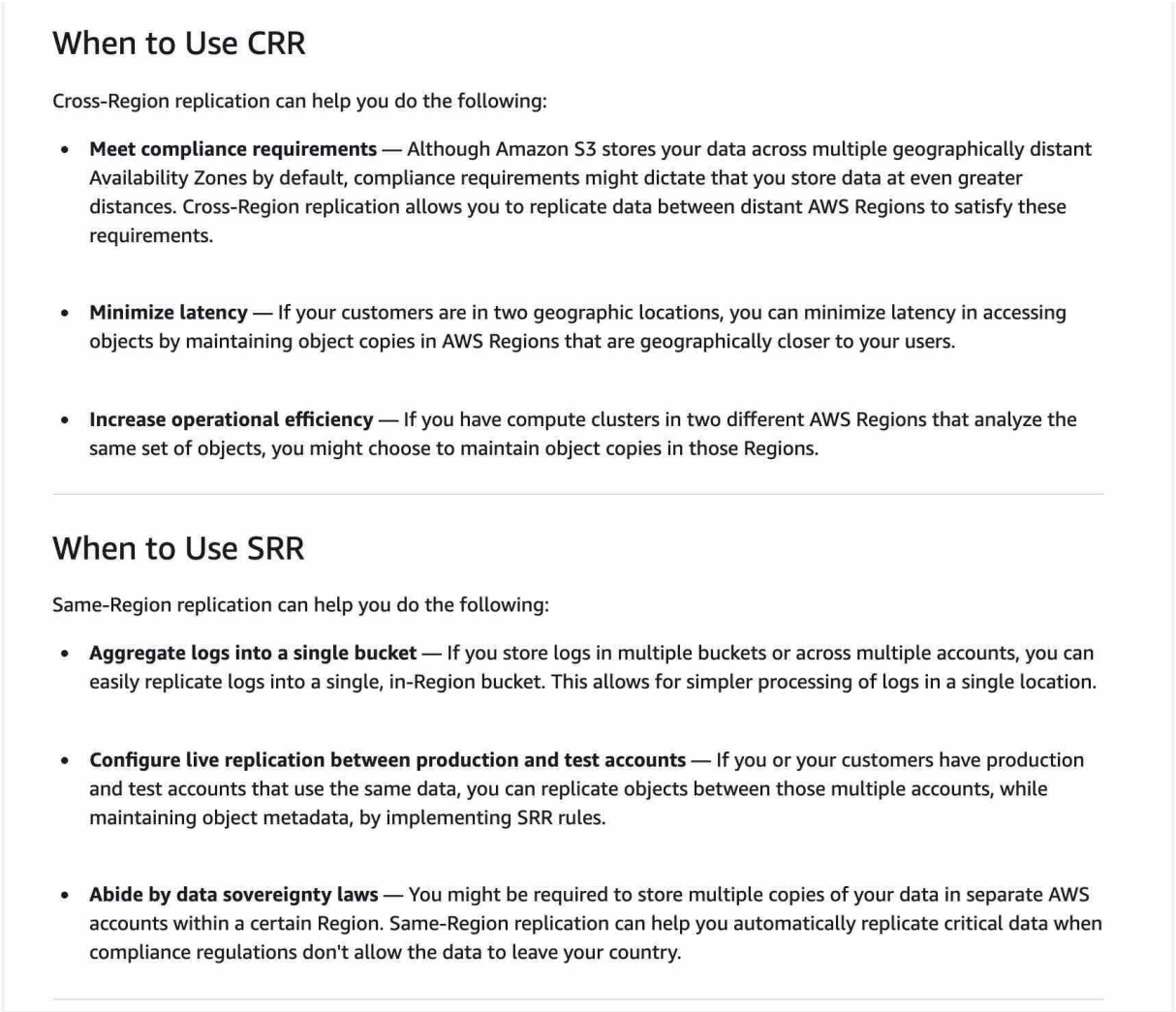
Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-Region Replication (CRR) allows you to replicate data between distant AWS Regions to satisfy these requirements.

Incorrect options:

Use Same-Region replication (SRR) to replicate data between distant AWS Regions - SRR is used to copy objects across Amazon S3 buckets in the same AWS Region, so this option is incorrect.

Exam Alert:

Please review the differences between SRR and
CRR:



When to Use CRR

Cross-Region replication can help you do the following:

- **Meet compliance requirements** — Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-Region replication allows you to replicate data between distant AWS Regions to satisfy these requirements.
- **Minimize latency** — If your customers are in two geographic locations, you can minimize latency in accessing objects by maintaining object copies in AWS Regions that are geographically closer to your users.
- **Increase operational efficiency** — If you have compute clusters in two different AWS Regions that analyze the same set of objects, you might choose to maintain object copies in those Regions.

When to Use SRR

Same-Region replication can help you do the following:

- **Aggregate logs into a single bucket** — If you store logs in multiple buckets or across multiple accounts, you can easily replicate logs into a single, in-Region bucket. This allows for simpler processing of logs in a single location.
- **Configure live replication between production and test accounts** — If you or your customers have production and test accounts that use the same data, you can replicate objects between those multiple accounts, while maintaining object metadata, by implementing SRR rules.
- **Abide by data sovereignty laws** — You might be required to store multiple copies of your data in separate AWS accounts within a certain Region. Same-Region replication can help you automatically replicate critical data when compliance regulations don't allow the data to leave your country.

via - https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html

For every new object, trigger a lambda function to write data into a bucket in another AWS Region - Although this solution is feasible, it's not resource efficient as the lambda is used to do something which S3 CRR can achieve off-the-shelf.

Run a daily job on an EC2 instance to copy objects into another Region - Creating a daily job on EC2 instance to copy objects into another Region involves a lot of development effort. It is much better to use S3 CRR for this task.

Reference:

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

Question 21: Correct
Which of the following is correct regarding the AWS Shield Advanced pricing?

Explanation
Correct option:

AWS Shield Advanced offers protection against higher fees that could result from a DDoS attack

AWS Shield Advanced offers some cost protection against spikes in your AWS bill that could result from a DDoS attack. This cost protection is provided for your Elastic Load Balancing load balancers, Amazon CloudFront distributions, Amazon Route 53 hosted zones, Amazon Elastic Compute Cloud instances, and your AWS Global Accelerator accelerators.

AWS Shield Advanced is a paid service for all customers, irrespective of the Support plan.

Incorrect options:

AWS Shield Advanced is a free service for AWS Enterprise Support plan

AWS Shield Advanced is a free service for AWS Business Support plan

AWS Shield Advanced is a free service for all AWS Support plans

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

Reference:

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

Question 22: Correct
Which AWS service will you use to privately connect your VPC to Amazon S3?

Explanation
Correct option:

VPC Endpoint Gateway

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 S3

DynamoDB

Exam Alert:

You may see a question around this concept in the exam. Just remember that only S3 and DynamoDB support VPC Endpoint Gateway. All other services that support VPC Endpoints use a VPC Endpoint Interface.

Incorrect options:

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. This private connection takes at least one month for completion.

AWS Transit Gateway - AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. This service is helpful in reducing the complex topology of VPC peering when a lot of systems are involved.

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.

Reference:

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

Question 23: **Correct**
An AWS user is trying to launch an EC2 instance in a given region. What is the region-specific constraint that the Amazon Machine Image (AMI) must meet so that it can be used for this EC2 instance?

- You should use an AMI from the same region, as it improves the performance of the EC2 instance
- An AMI is a global entity, so the region is not applicable
- You can use an AMI from a different region, but it degrades the performance of the EC2 instance
- You must use an AMI from the same region as that of the EC2 instance. The region of the AMI has no bearing on the performance of the EC2 instance **(Correct)**

Explanation
Correct option:

You must use an AMI from the same region as that of the EC2 instance. The region of the AMI has no bearing on the performance of the EC2 instance

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

The AMI must be in the same region as that of the EC2 instance to be launched. If the AMI exists in a different region, you can copy that AMI to the region where you want to launch the EC2 instance. The region of AMI has no bearing on the performance of the EC2 instance.

Amazon Machine Images (AMI)
Overview:

Amazon Machine Images (AMI)

PDF | Kindle | RSS

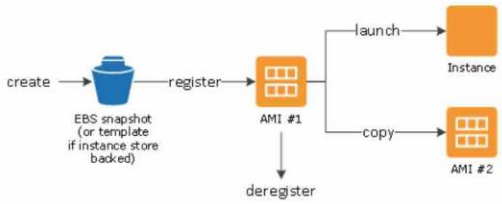
An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances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

An AMI includes the following:

- One or more EBS snapshots, or, for instance-store-backed AMIs, a template for the root volume of the instance (for example, an operating system, an application server, and applications).
- Launch permissions that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the volumes to attach to the instance when it's launched.

Using an AMI

The following diagram summarizes the AMI lifecycle. After you create and register an AMI, you can use it to launch new instances. (You can also launch instances from an AMI if the AMI owner grants you launch permissions.) You can copy an AMI within the same Region or to different Regions. When you no longer require an AMI, you can deregister it.



You can search for an AMI that meets the criteria for your instance. You can search for AMIs provided by AWS or AMIs provided by the community. For more information, see AMI types and Finding a Linux AMI.

After you launch an instance from an AMI, you can connect to it. When you are connected to an instance, you can use it just like you use any other server. For information about launching, connecting, and using your instance, see Amazon EC2 instances.

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

Incorrect options:

You can use an AMI from a different region, but it degrades the performance of the EC2 instance

You should use an AMI from the same region, as it improves the performance of the EC2 instance

An AMI is a global entity, so the region is not applicable

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

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

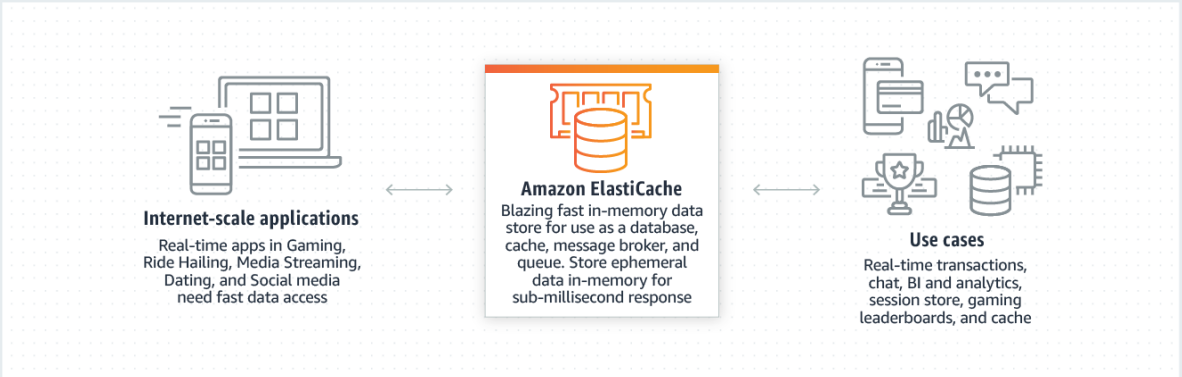
Question 24:
Which AWS service can be used as an in-memory database with high-performance and low latency?

Explanation
Correct option:

Amazon ElastiCache

Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-Source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for real-time use cases like Caching, Session Stores, Gaming, Geospatial Services, Real-Time Analytics, and Queuing. ElastiCache cannot be used for online analytical processing.

How ElastiCache Works:



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

Incorrect options:

Amazon RDS - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. RDS cannot be used as an in-memory database.

Amazon DynamoDB - Amazon DynamoDB is a NoSQL database that supports key-value and document data models and enables developers to build modern, serverless applications that can start small and scale globally to support petabytes of data and tens of millions of read and write requests per second. DynamoDB supports both key-value and document data models. This enables DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases. DynamoDB cannot be used as an in-memory database.

Amazon Athena - Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. Athena cannot be used as an in-memory database.

Reference:

https://aws.amazon.com/elasticache/

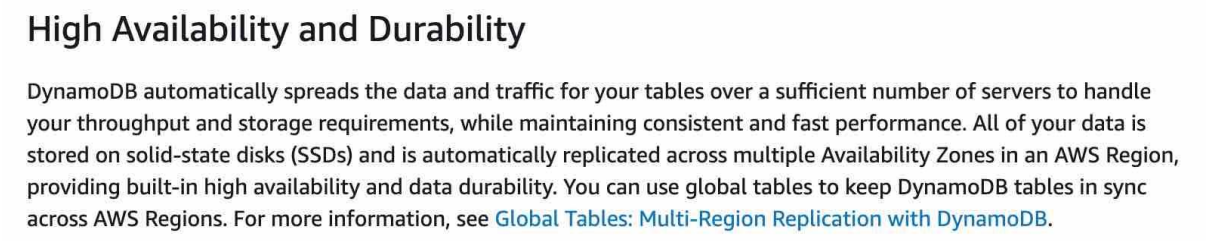
Question 25: **Incorrect**
Which AWS services support High Availability by default? (Select two)

- ☐

Explanation
Correct options:

DynamoDB - Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-Region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in high availability and data durability.

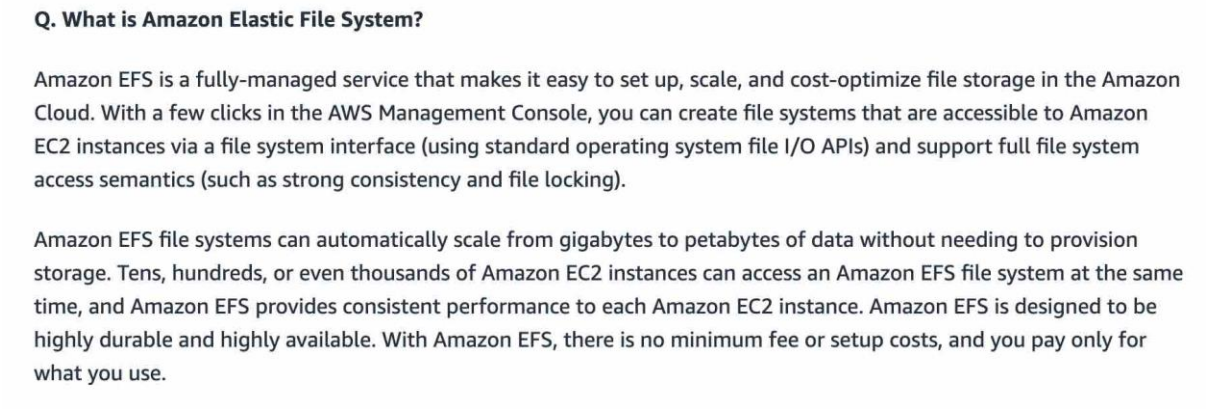
DynamoDB High
Availability:



via
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

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. Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability.

EFS High
Availability:



Q. What is Amazon Elastic File System?

Amazon EFS is a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and support full file system access semantics (such as strong consistency and file locking).

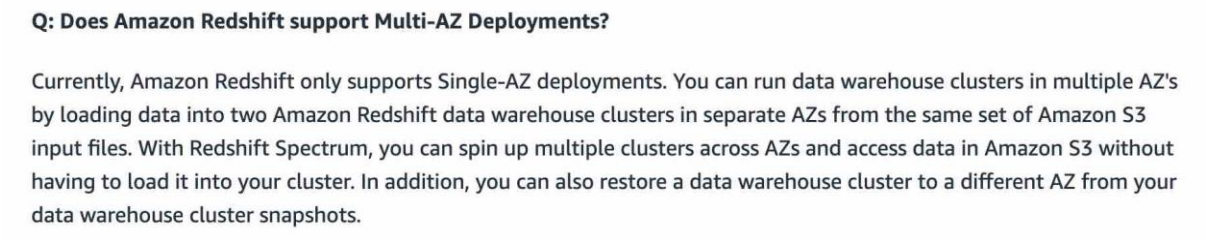
Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available. With Amazon EFS, there is no minimum fee or setup costs, and you pay only for what you use.

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

Incorrect options:

Redshift - Amazon Redshift is a fast, fully managed cloud data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools.

Amazon Redshift only supports Single-AZ
deployments:



Q: Does Amazon Redshift support Multi-AZ Deployments?

Currently, Amazon Redshift only supports Single-AZ deployments. You can run data warehouse clusters in multiple AZ's by loading data into two Amazon Redshift data warehouse clusters in separate AZs from the same set of Amazon S3 input files. With Redshift Spectrum, you can spin up multiple clusters across AZs and access data in Amazon S3 without having to load it into your cluster. In addition, you can also restore a data warehouse cluster to a different AZ from your data warehouse cluster snapshots.

via - https://aws.amazon.com/redshift/faqs/

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 are replicated within an Availability Zone (AZ) and can easily scale to petabytes of data.

Instance Store - As Instance Store volumes are tied to an EC2 instance, they are also single AZ entities.

References:

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

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

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

https://aws.amazon.com/ebs/

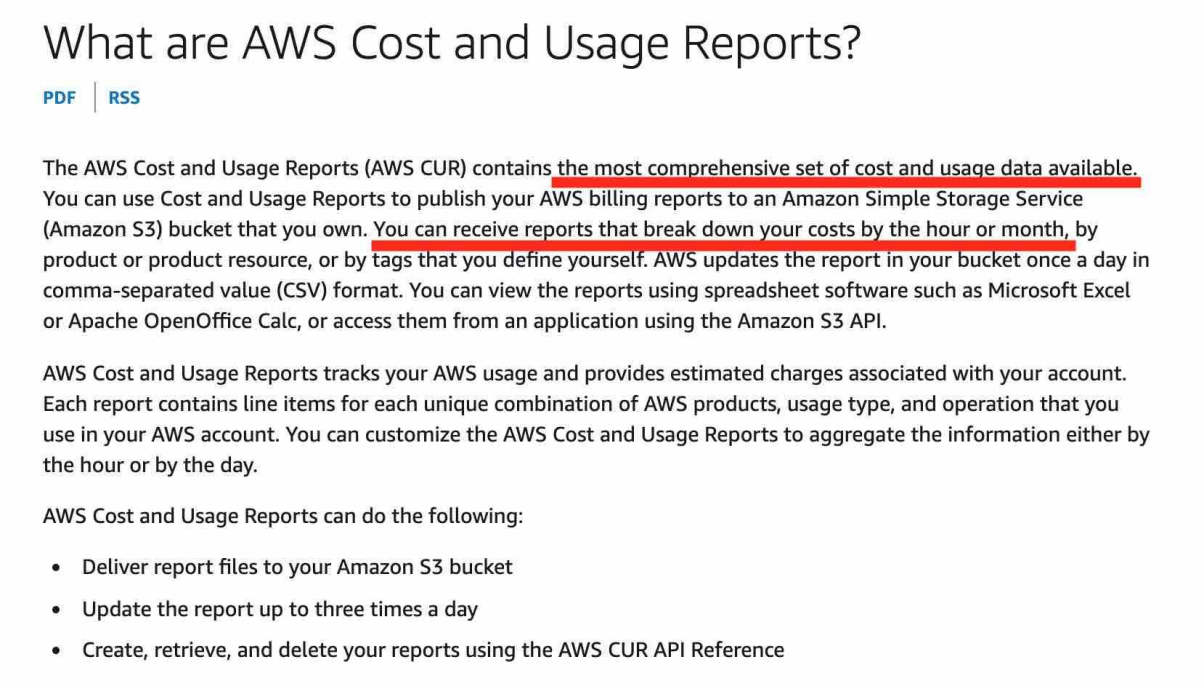
Question 26:
A startup wants to set up its IT infrastructure on AWS Cloud. The CTO would like to receive detailed reports that break down the startup's AWS costs by the hour in an S3 bucket. As a Cloud Practitioner, which AWS service would you recommend for this use-case?

Explanation
Correct option:

AWS Cost and Usage Reports

The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself. AWS updates the report in your bucket once a day in comma-separated value (CSV) format.

AWS Cost and Usage Reports
Overview:



What are AWS Cost and Usage Reports?

PDF | RSS

The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself. AWS updates the report in your bucket once a day in comma-separated value (CSV) format. You can view the reports using spreadsheet software such as Microsoft Excel or Apache OpenOffice Calc, or access them from an application using the Amazon S3 API.

AWS Cost and Usage Reports tracks your AWS usage and provides estimated charges associated with your account. Each report contains line items for each unique combination of AWS products, usage type, and operation that you use in your AWS account. You can customize the AWS Cost and Usage Reports to aggregate the information either by the hour or by the day.

AWS Cost and Usage Reports can do the following:

- Deliver report files to your Amazon S3 bucket
- Update the report up to three times a day
- Create, retrieve, and delete your reports using the AWS CUR API Reference

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

Incorrect options:

AWS Total Cost of Ownership (TCO) Calculator - TCO calculator helps to compare the cost of your applications in an on-premises or traditional hosting environment to AWS. AWS helps reduce Total Cost of Ownership (TCO) by reducing the need to invest in large capital expenditures and providing a pay-as-you-go model that empowers to invest in the capacity you need and use it only when the business requires it. Once you describe your on-premises or hosting environment configuration, it produces a detailed cost comparison with AWS.

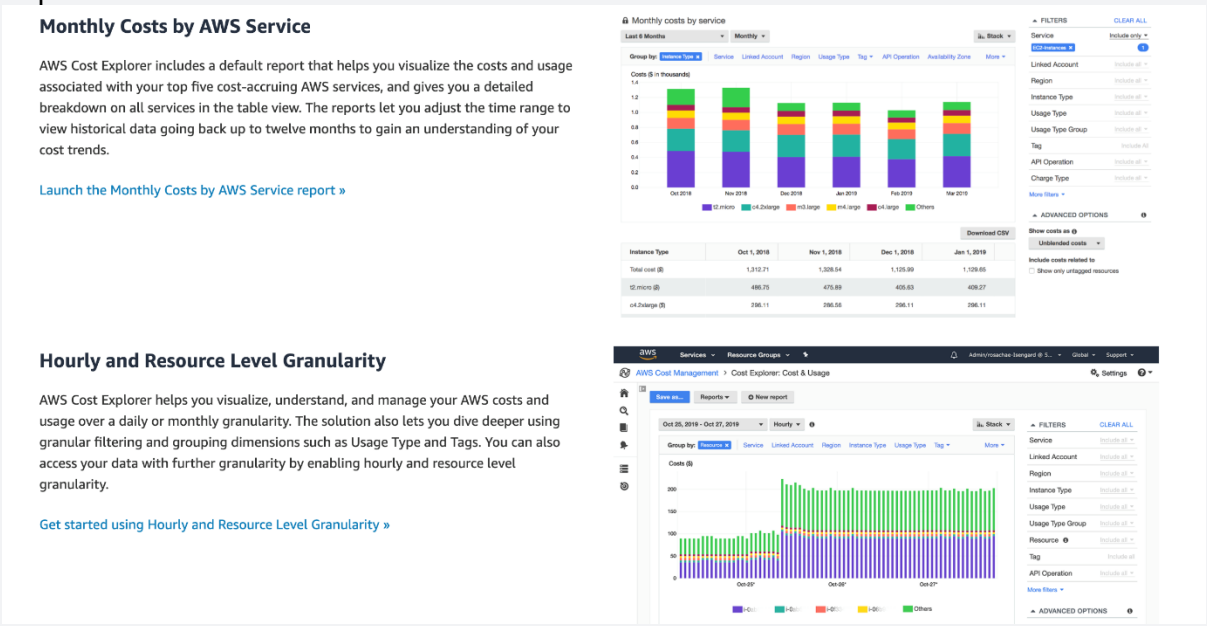
AWS Cost Explorer - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and 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 a detailed report of your AWS costs by the hour into an S3 bucket.

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. AWS Budgets cannot provide a detailed break down of your AWS costs by the hour.

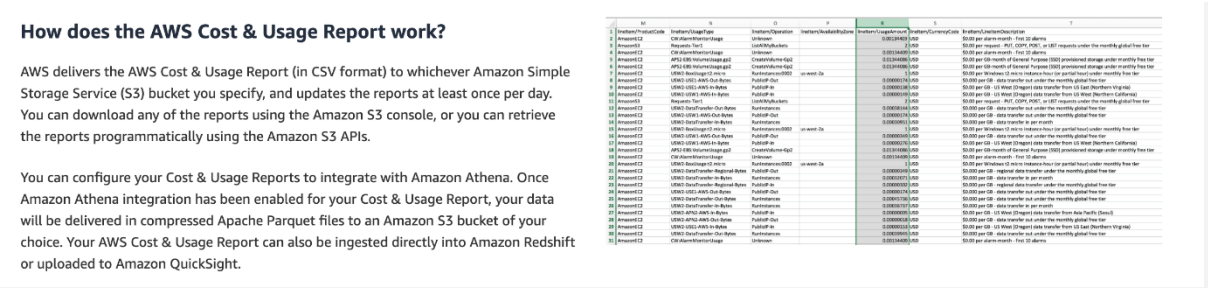
Exam Alert:

Please review the differences between "AWS Cost and Usage Reports" and "AWS Cost Explorer". Think of "AWS Cost and Usage Reports" as a cost management tool providing the most detailed cost and usage data for your AWS account. It can provide reports that break down your costs by the hour into your S3 bucket. On the other hand, "AWS Cost Explorer" is more of a high-level cost management tool that helps you visualize the costs and usage associated with your AWS account.

"AWS Cost Explorer" vs "AWS Cost and Usage Reports":



via - https://aws.amazon.com/aws-cost-management/aws-cost-explorer/



via - https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/

References:

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

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

https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/

Question 27: Correct
Which of the following statements are CORRECT regarding Security Groups and Network Access Control Lists (NACLs)? (Select two)

- ☐ A Security Group contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic
- ☐ A Security Group is stateless, that is, the return traffic must be explicitly allowed
- ☑ A Security Group is stateful, that is, it automatically allows the return traffic **(Correct)**
- ☐ A NACL is stateful, that is, it automatically allows the return traffic
- ☑ A NACL contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic **(Correct)**

Explanation
Correct options:

A Security Group is stateful, that is, it automatically allows the return traffic

A NACL contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic

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. 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. A security group evaluates all rules before deciding whether to allow 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 (NACL) 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 contains a numbered list of rules. A NACL evaluates 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. AWS recommends 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.

Network Access Control List (NACL)
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

Incorrect options:

A Security Group contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic

A NACL is stateful, that is, it automatically allows the return traffic

A Security Group is stateless, that is, the return traffic must be explicitly allowed

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

Question 28:
Which S3 storage class offers the lowest availability?

Explanation
Correct option:

S3 One Zone-IA

S3 One Zone-IA is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ.

Please review this illustration for S3 Storage Classes availability. You don't need to memorize the actual numbers, just remember that S3 One Zone-IA offers the lowest availability:

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

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

Incorrect options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data.

S3 Intelligent-Tiering - The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. 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 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.

References:

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

Question 29: Correct
Under the AWS Shared Responsibility Model, which of the following is the responsibility of a customer regarding lambda functions?

- Patch underlying OS for the lambda function infrastructure
- Maintain versions of a lambda function **(Correct)**
- Maintain all runtime environments for lambda functions
- Configure networking infrastructure for the lambda functions

Explanation
Correct option:

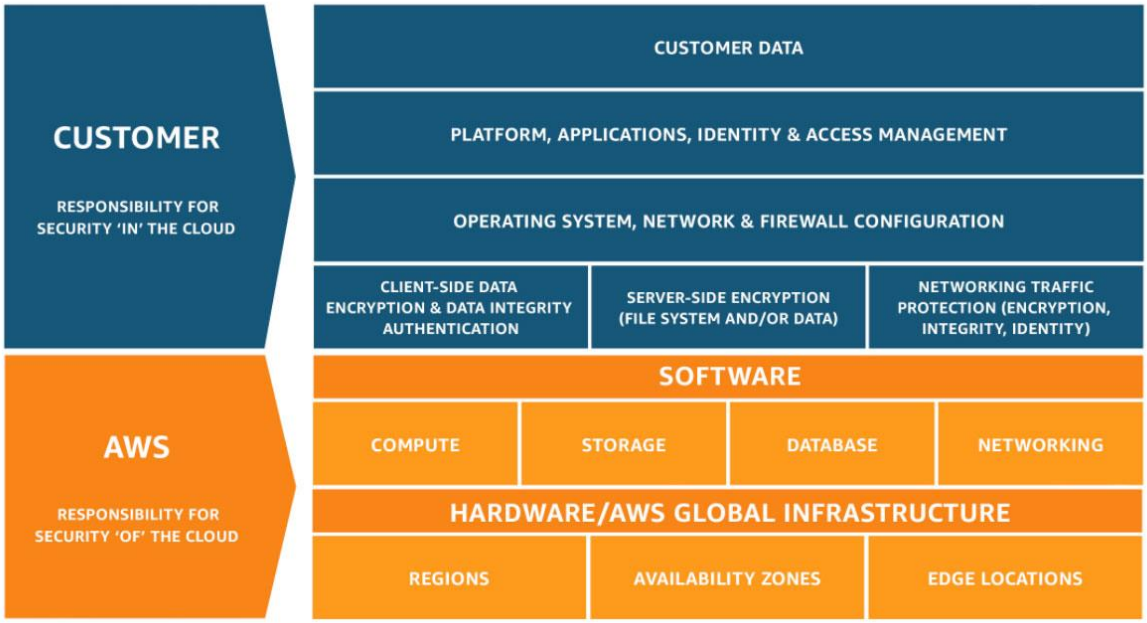
Maintain versions of a lambda function

Under the Shared Responsibility Model, 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.

Under the Shared Responsibility Model, Customer's responsibility is determined by the AWS Cloud services that a customer selects. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

For the given use-case, the customer is responsible for maintaining the versions of a lambda function.

Shared Responsibility Model
Overview:



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

Incorrect options:

Patch underlying OS for the lambda function infrastructure

Maintain all runtime environments for lambda functions

Configure networking infrastructure for the lambda functions

As mentioned earlier, all these options fall under the ambit of AWS as far as the Shared Responsibility Model is concerned.

Reference:

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

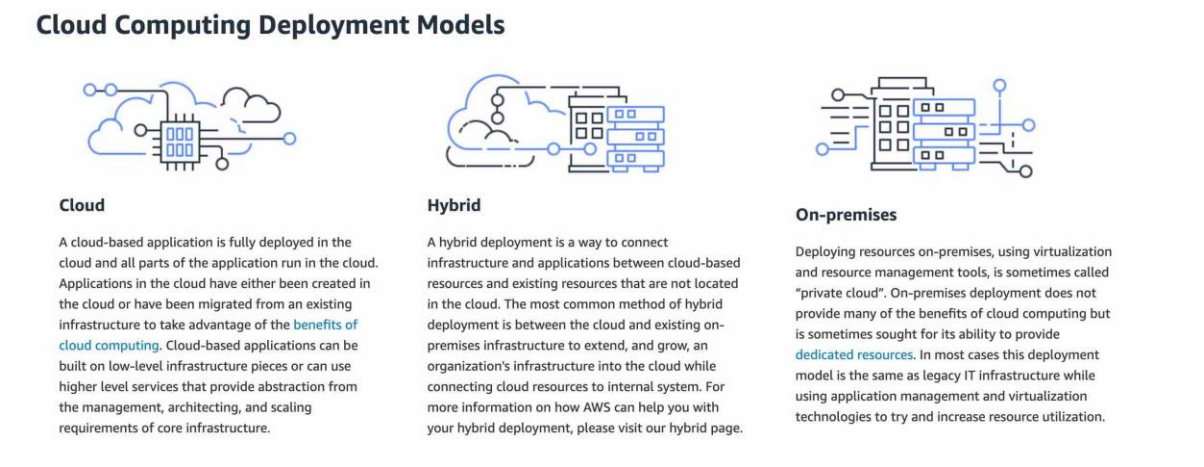
Question 30: Correct
Enterprise environments are often a mix of cloud, on-premises data centers, and edge locations. Which Cloud deployment model does this refer to?

Explanation
Correct option:

Hybrid Cloud

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

Overview of Cloud Computing Deployment Models:



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

Incorrect options:

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

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

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

Reference:

https://aws.amazon.com/what-is-cloud-computing/

Question 31: Correct
Which of the following AWS services is an example of Software as a Service (SaaS)?

- AWS Elastic Beanstalk
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Simple Storage Service (Amazon S3) **(Correct)**
-

AWS Storage Gateway

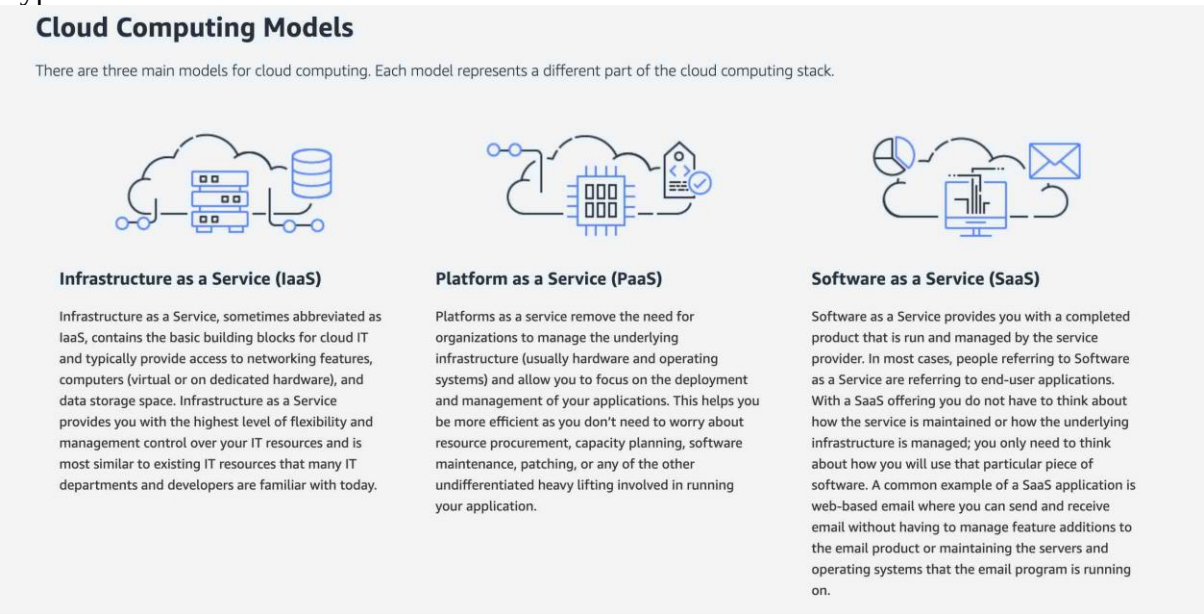
Explanation
Correct option:

Amazon Simple Storage Service (Amazon S3)

Software as a Service (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.

Amazon Simple Storage Service (Amazon S3) - Amazon S3 can be used for storing data directly without having to do anything with underlying infrastructure, maintenance or deployments. S3 is an example of a storage service that can be categorized as Software as a Service (SaaS).

Overview of Cloud Computing
Types:



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

Incorrect options:

Infrastructure as a Service (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.

Platform as a Service (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.

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. EC2 provides compute capacity and maintenance of guest Operating systems, patches and deployment of code is the responsibility of the customer. So, EC2 comes under Infrastructure as a Service (IaaS).

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. You use the AWS Management Console to download the virtual appliance gateway or purchase the hardware appliance, hence it does not fall under Software as a Service model.

**AWS Elastic Beanstalk ** - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with a wide range of programming languages. You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. This service falls under Platform as a Service (PaaS).

Reference:

https://aws.amazon.com/what-is-cloud-computing/

Question 32: Correct
Which AWS service can help you forecast your next AWS bill for the services you use?

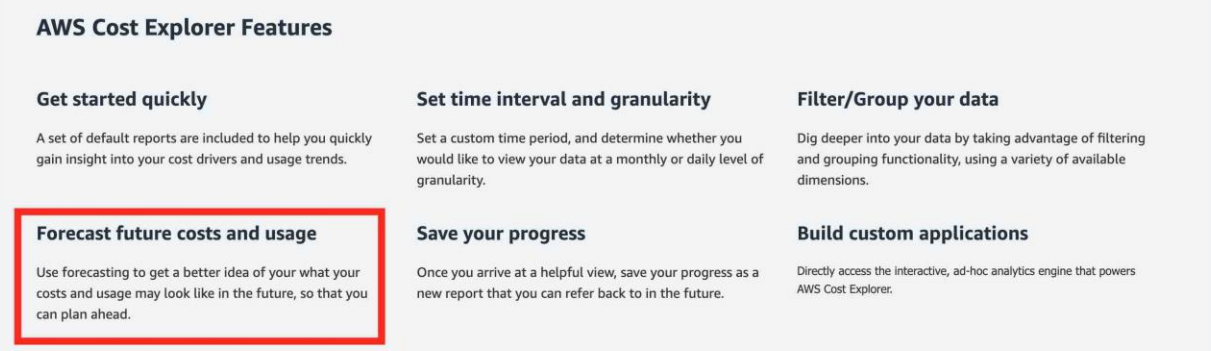
Explanation
Correct option:

AWS Cost Explorer

A forecast is a prediction of how much you will use AWS services over the forecast time period that you selected, based on your past usage. Forecasting provides an estimate of what your AWS bill will be and enables you to use alarms and budgets for amounts that you're predicted to use.

AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. At the top of the Cost Explorer page are the Month-to-date costs and Forecasted month end costs. The Forecasted month end costs show how much Cost Explorer estimates that you will owe at the end of the month and compares your estimates costs to your actual costs of the previous month.

AWS Cost Explorer
Features:



via - https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-exploring-data.html

Incorrect options:

AWS Simple Monthly Calculator - The Simple Monthly 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.

AWS Total Cost of Ownership (TCO) Calculator - To estimate the costs of migrating on-premises infrastructure to AWS, you use the AWS Total Cost of Ownership (TCO) Calculator. The calculator can be accessed from https://awstcocalculator.com/. You cannot use this service to forecast your next AWS bill.

AWS Billing and Cost Management - AWS Billing and Cost Management is the service that you use to pay your AWS bill, monitor your usage, and analyze and control your costs. It is the billing department for AWS services - with necessary tools and services under its hood. You cannot use this service to forecast your next AWS bill.

Reference:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-exploring-data.html

Question 33: Correct
Which of the following capabilities does Amazon Rekognition provide as a ready-to-use feature?

Explanation
Correct option:

Identify objects in a photo

With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.

Amazon Rekognition Use-Cases:

Key features

Labels

With Amazon Rekognition, you can identify thousands of objects (such as bike, telephone, building), and scenes (such as parking lot, beach, city). When analyzing video, you can also identify specific activities such as "delivering a package" or "playing soccer". Learn more »

Custom labels

With Amazon Rekognition Custom Labels, you can extend the detection capabilities of Amazon Rekognition to extract information from images that is uniquely helpful to your business. For example, you can find your corporate logo in social media, identify your products on store shelves, classify your machine parts in an assembly line, or detect your animated characters in videos. Learn more »

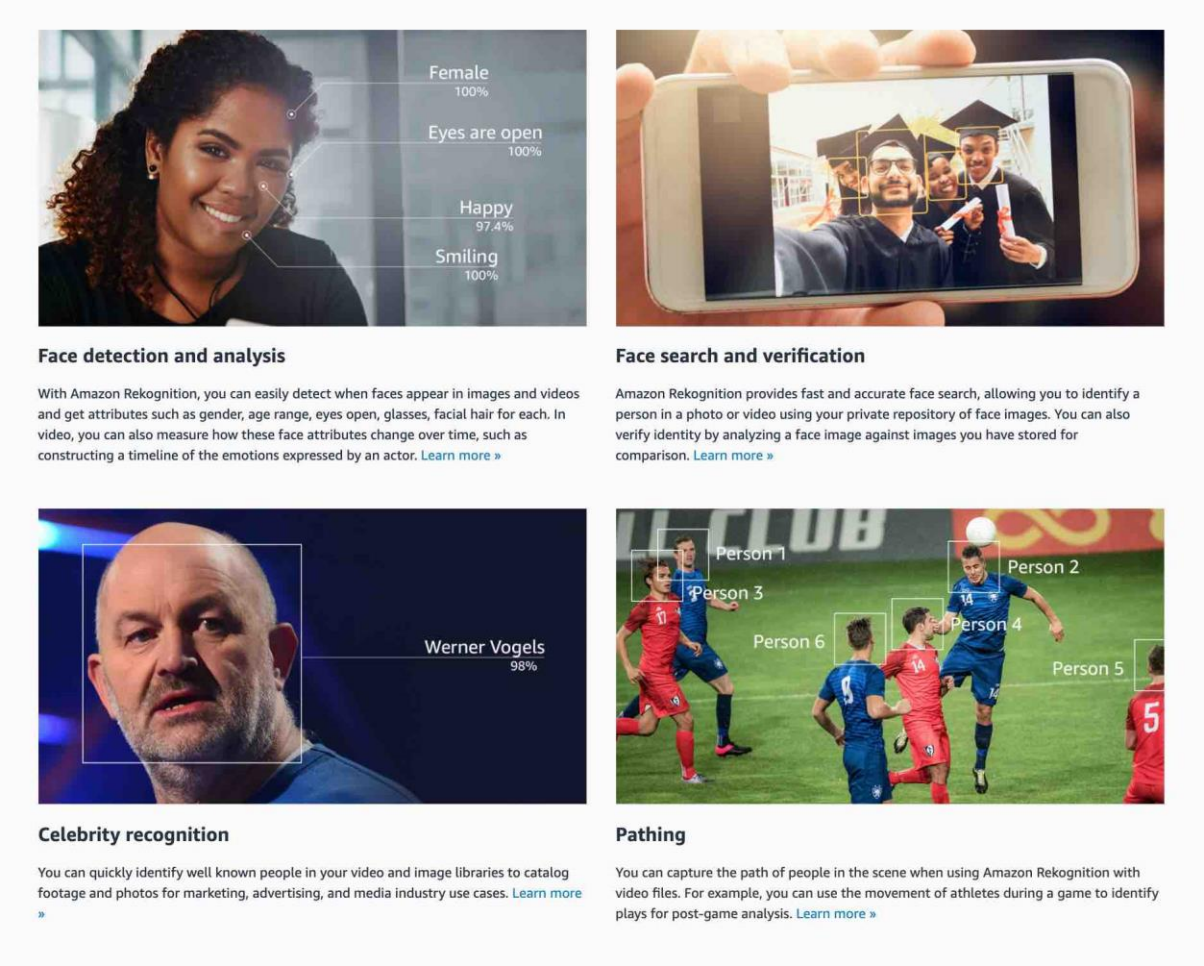
Content moderation

Amazon Rekognition helps you identify potentially unsafe or inappropriate content across both image and video assets and provides you with detailed labels that allow you to accurately control what you want to allow based on your needs. Use Amazon A2I to enhance the accuracy of Amazon Rekognition image moderation predictions using human review. Learn more »

Text detection

In photos and videos, text appears very differently than neat words on a printed page. Amazon Rekognition can read skewed and distorted text to capture information like store names, forced narratives overlaid on media, street signs, and text on product packaging. Learn more »

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



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

Incorrect options:

Convert images into greyscale

Resize images quickly

Human pose detection

Amazon Rekognition does not do image processing tasks such as converting images to greyscale or resizing images. Human pose detection is not available in Amazon Rekognition.

Reference:

Question 34:
According to the AWS Shared Responsibility Model, which of the following are responsibilities of the customer (select 2)?

- ☐

Explanation
Correct options:

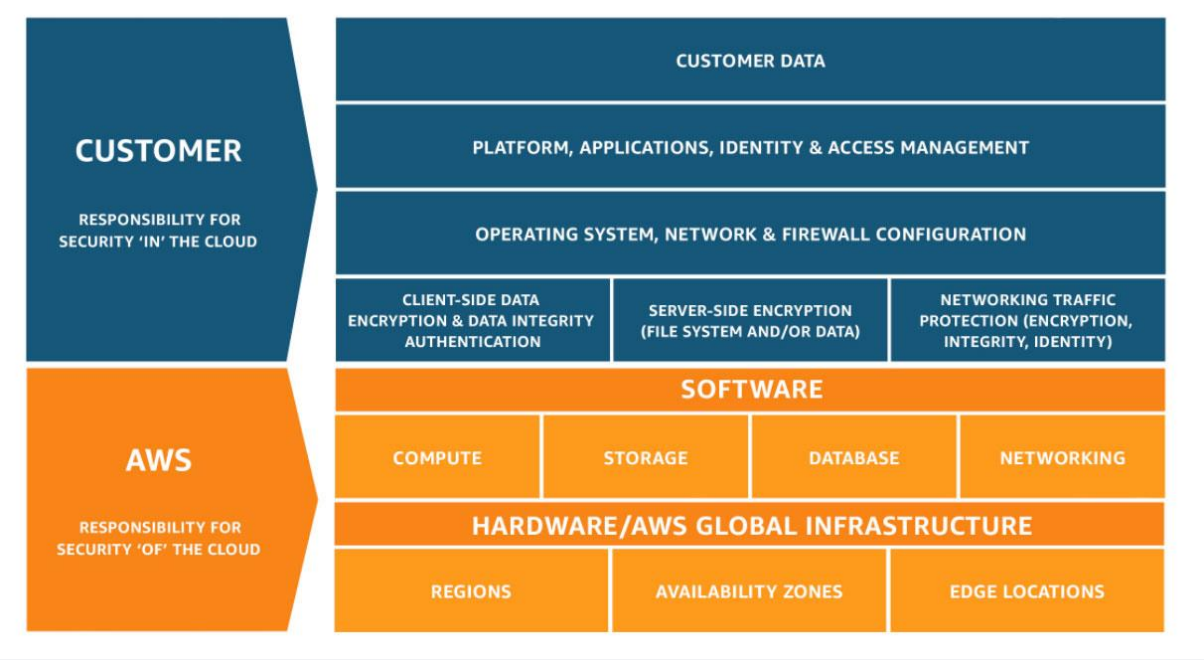
Under the Shared Responsibility Model, AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Customer's responsibility is determined by the AWS Cloud services that a customer selects.

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.

Operating system patches and updates of an EC2 instance - Security "in" the cloud is the responsibility of the customer. A service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks.

Enabling data encryption of data stored in S3 buckets - In the Shared Responsibility Model, customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

Shared Responsibility Model
Overview:



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

Incorrect options:

AWS Global Network Security - Cloud infrastructure management is the responsibility of AWS.

Ensuring AWS employees cannot access customer data - Ensuring protection of customer data and keeping it safe from AWS employees is the responsibility of AWS.

Compliance validation of Cloud infrastructure - Cloud security and compliance are the responsibilities of AWS.

Reference:

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

Question 35: **Correct**
Which of the following improves the availability for a fleet of EC2 instances?

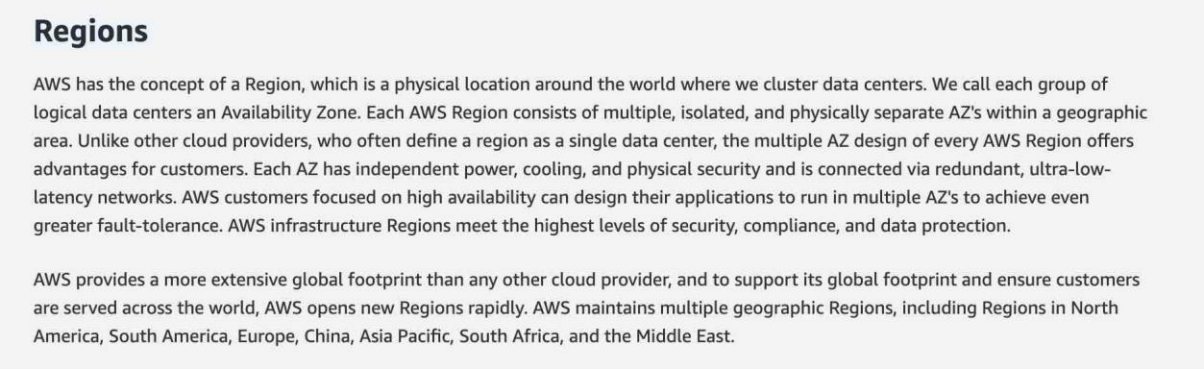
Explanation
Correct option:

Deploy the EC2 instances across different Availability Zones in the same AWS Region

AWS has the concept of a Region, which is a physical location around the world where AWS clusters data centers. Each AWS Region consists of multiple (two or more), isolated, and physically separate AZ's 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. An AWS Region refers to a physical location around the world where AWS clusters data centers. AZ's give customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data center. All AZ's 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 AZ's.

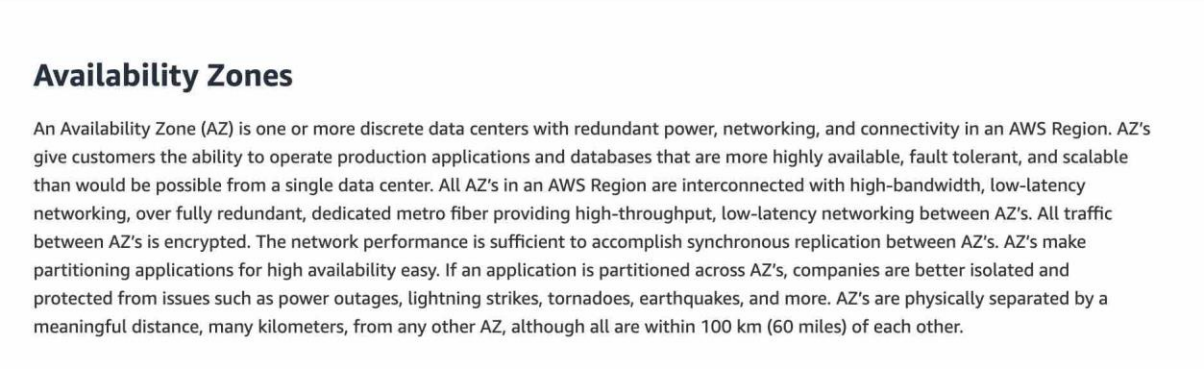
AWS Regions and Availability Zones
Explained:



Regions

AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. We call each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area. Unlike other cloud providers, who often define a region as a single data center, the multiple AZ design of every AWS Region offers advantages for customers. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZ's to achieve even greater fault-tolerance. AWS infrastructure Regions meet the highest levels of security, compliance, and data protection.

AWS provides a more extensive global footprint than any other cloud provider, and to support its global footprint and ensure customers are served across the world, AWS opens new Regions rapidly. AWS maintains multiple geographic Regions, including Regions in North America, South America, Europe, China, Asia Pacific, South Africa, and the Middle East.



Availability Zones

An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. AZ's give customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data center. All AZ's 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 AZ's. All traffic between AZ's is encrypted. The network performance is sufficient to accomplish synchronous replication between AZ's. AZ's make partitioning applications for high availability easy. If an application is partitioned across AZ's, companies are better isolated and protected from issues such as power outages, lightning strikes, tornadoes, earthquakes, and more. AZ's are physically separated by a meaningful distance, many kilometers, from any other AZ, although all are within 100 km (60 miles) of each other.

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

Incorrect options:

Deploy the EC2 instances in the same Availability Zone of an AWS Region - Deploying EC2 instances within the same AZ will not improve availability.

Deploy the EC2 instances in the same Availability Zone across two different AWS Regions - An Availability Zone cannot belong to two different AWS Regions. So this option is incorrect.

Deploy the EC2 instances across different AWS Regions of the same Availability Zone - You cannot have an AWS Region inside an Availability Zone. So this option is incorrect.

Reference:

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

Question 36:
An IT company is on a cost-optimization spree and wants to identify all EC2 instances that are under-utilized. Which AWS service can be used to address this use-case?

Explanation
Correct option:

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

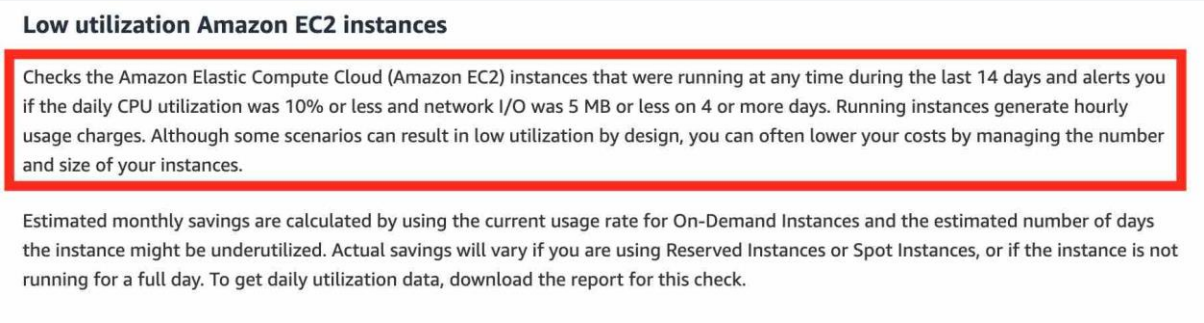
Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

AWS Trusted Advisor checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days.

How Trusted Advisor Works:

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

How AWS Trusted Advisor identifies low utilization Amazon EC2 instances:



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

Incorrect options:

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. Cost Explorer cannot be used to identify under-utilized EC2 instances.

AWS Cost and Usage Reports - The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself. Cost and Usage Reports cannot be used to identify under-utilized EC2 instances.

Amazon CloudWatch - Amazon CloudWatch can be used to create alarm to monitor your estimated charges. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data. You can choose to receive alerts by email when charges have exceeded a certain threshold. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot be used to identify under-utilized EC2 instances.

Reference:

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

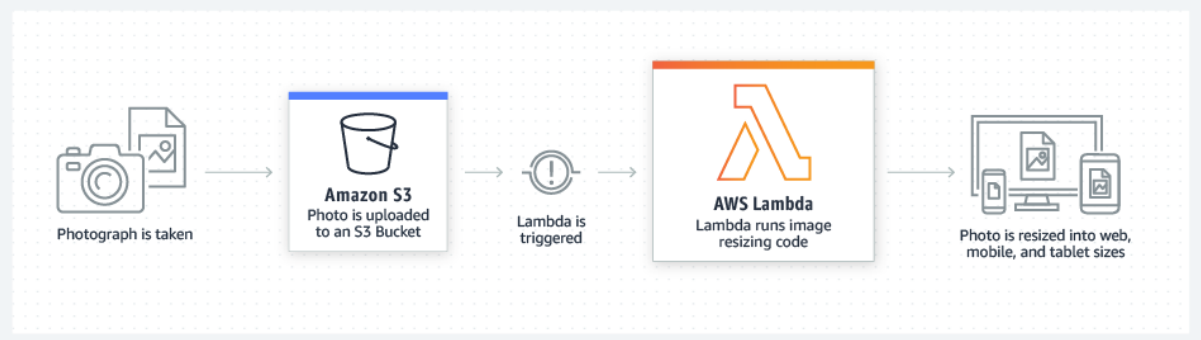
Question 37:
Which AWS service can be used to execute code triggered by new files being uploaded to S3?

Explanation
Correct option:

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.

You can use Amazon S3 to trigger AWS Lambda to process data immediately after an upload. For example, you can use Lambda to thumbnail images, transcode videos, index files, process logs, validate content, and aggregate and filter data in real-time.

How Lambda executes code in response to a trigger from S3:



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

Incorrect options:

EC2 - 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. EC2 cannot execute code via a trigger from S3.

ECS - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster. ECS cannot execute code via a trigger from S3.

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.

Although SQS can be triggered from an S3 event, but SQS cannot execute code as its a message queuing service.

Reference:

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

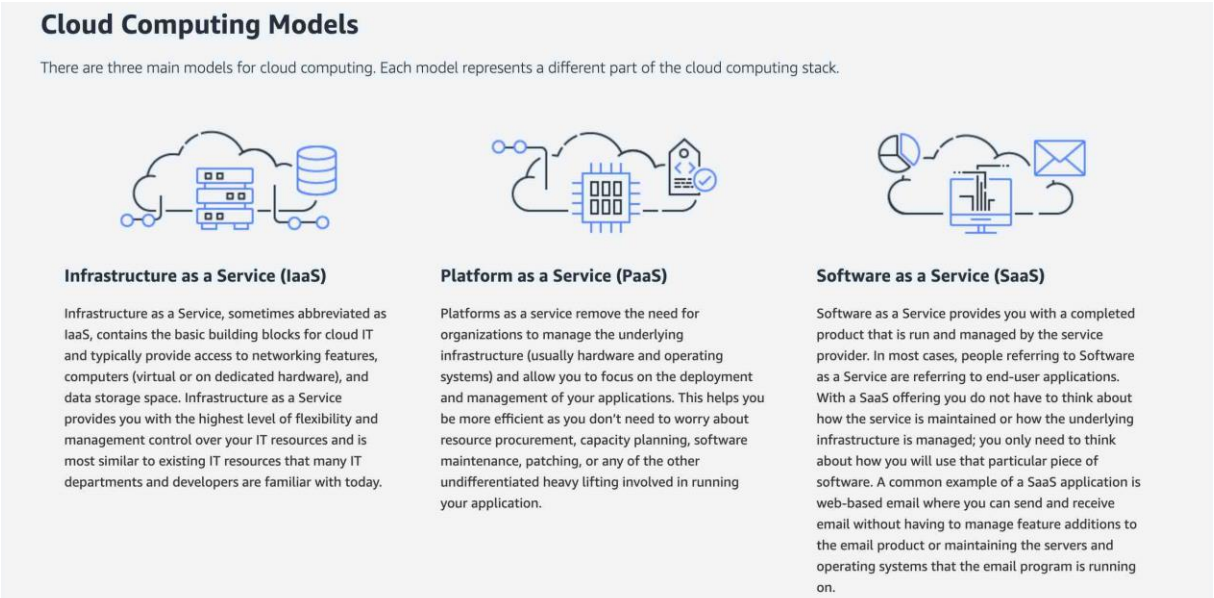
Question 38: **Correct**
Gmail is an example of which of the following Cloud Computing Models?

Explanation
Correct option:

Software as a Service (SaaS)

Software as a Service (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. Gmail is an example of a SaaS service.

Overview of Cloud Computing
Types:



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

Incorrect options:

Infrastructure as a Service (IaaS) - Infrastructure as a Service (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 is an example of an IaaS service.

Platform as a Service (PaaS) - Platform as a Service (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. Beanstalk is an example of a PaaS service.

Function as a Service (FaaS) - Function as a service (FaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage application functionalities without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. Lambda is an example of a FaaS service.

Reference:

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

Question 39: Correct
Which of the following AWS services are regional in scope? (Select two)

- ☐
- ☐
- ☐ Amazon CloudFront

Explanation

Correct options:

Most of the services that AWS offers are Region specific. But few services, by definition, need to be in a global scope because of the underlying service they offer. AWS IAM, Amazon CloudFront, Route 53 and WAF are some of the global services.

AWS Lambda - AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. Lambda is a regional service.

Amazon Rekognition - With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases. Rekognition is a regional service.

Incorrect options:

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

Amazon CloudFront - Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

AWS WAF - By using AWS WAF, you can configure web access control lists (Web ACLs) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures.

As mentioned earlier, these three services are global in scope.

Exam Alert:

Amazon S3 - Amazon S3 is a unique service in the sense that it follows a global namespace but the buckets are regional. You specify an AWS Region when you create your Amazon S3 bucket. This is a regional service.

Question 40: **Correct**
Which AWS Support plan guarantees a case response time of 15 minutes when Business Critical systems are down?

Explanation
Correct option:

Enterprise - 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. This plan provides Enhanced Technical Support as follows:

24x7 access to Cloud Support Engineers via phone, chat, and email. You can have an unlimited number of contacts that can open an unlimited amount of cases. Response times are as follows:

General Guidance - < 24 hours

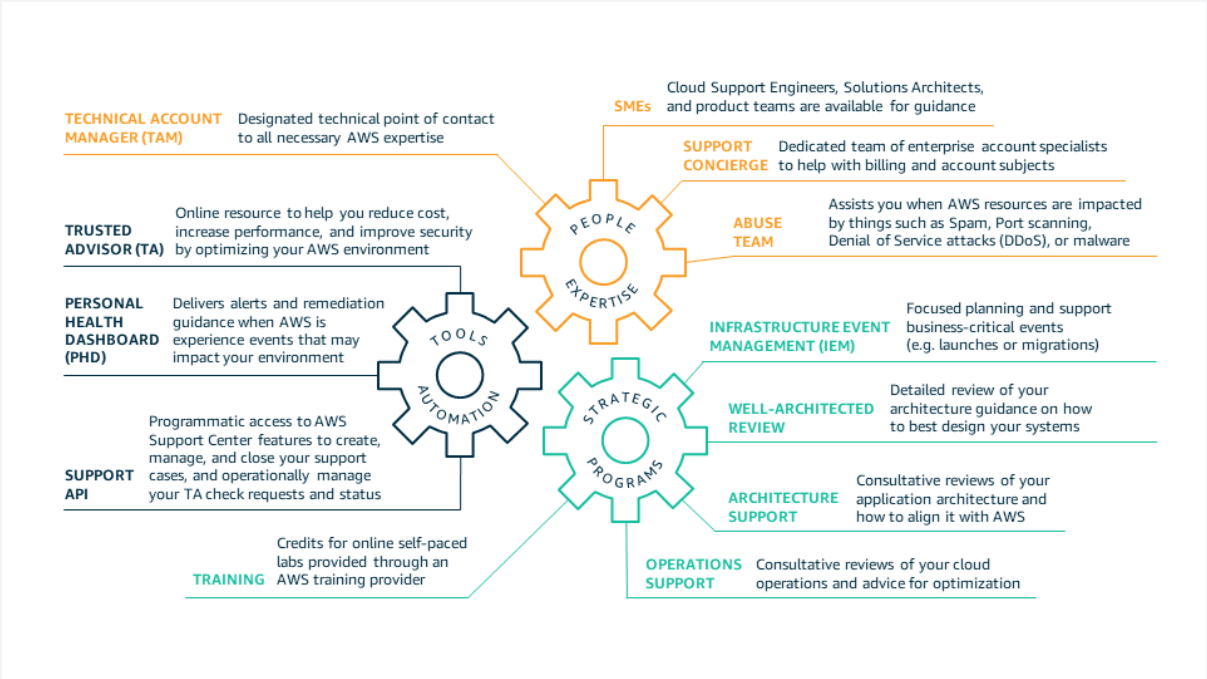
System Impaired - < 12 hours

Production System Impaired - < 4 hours

Production System Down - < 1 hour

Business Critical System Down - <15 min

Benefits of AWS Enterprise Support Plan:



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

Incorrect options:

Business - AWS recommends 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. This plan does not guarantee any specific response time for Business Critical systems.

Developer - AWS recommends 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. You do not get access to Infrastructure Event Management with this plan. This plan does not guarantee any specific response time for Business Critical systems.

Basic - The basic 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 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted. This plan does not guarantee any specific response time for Business Critical systems.

Reference:

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

Question 41:
Amazon Macie discovers and protects your sensitive data on which of the following AWS services?

Explanation
Correct option:

Amazon Simple Storage Service (Amazon S3)

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).

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). Macie is not integrated with EBS.

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. Macie is not integrated with EFS.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Macie is not integrated with Storage Gateway.

Reference:

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

Question 42: Correct
Which pillar of the AWS Well-Architected Framework recommends maintaining infrastructure as code?
Explanation
Correct option:

Operational Excellence

The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement.

The AWS Well-Architected Framework is based on five pillars — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.

The Operational Excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events.

Incorrect options:

Cost Optimization - Cost Optimization focuses on avoiding un-needed costs. Key topics include understanding and controlling where the money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.

Performance Efficiency - The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

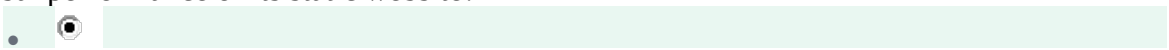
Security - The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

Reference:

https://wa.aws.amazon.com/wat.pillar.operationalExcellence.en.html

Question 43:

A company has a static website hosted on an S3 bucket in an AWS Region in Asia. Although most of its users are in Asia, now it wants to drive growth globally. How can it improve the global performance of its static website?



Explanation
Correct option:

Use CloudFront to improve the performance of your website

You can use Amazon CloudFront to improve the performance of your website. CloudFront makes your website files (such as HTML, images, and video) available from data centers around the world (called edge locations). When a visitor requests a file from your website, CloudFront automatically redirects the request to a copy of the file at the nearest edge location. This results in faster download times than if the visitor had requested the content from a data center that is located farther away.

Incorrect options:

Use CloudFormation to improve the performance of your website - 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 cannot be used to improve the performance of a static website.

Use WAF to improve the performance of your website - By using AWS WAF, you can configure web access control lists (Web ACLs) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures. Besides, by using AWS WAF's rate-based rules, you can automatically block the IP addresses of bad actors when requests matching a rule exceed a threshold that you define. WAF cannot be used to improve the performance of a static website.

Use S3 Transfer Acceleration to improve the performance of your website - Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path. Transfer Acceleration cannot be used to improve the performance of a static website.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-cloudfront-walkthrough.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

Question 44: **Correct**
An IT company has a hybrid cloud architecture and it wants to centralize the server logs for its EC2 instances and on-premises servers. Which of the following is the MOST effective for this use-case?

Explanation
Correct option:

Use CloudWatch Logs for both the EC2 instance and the on-premises servers

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources such as on-premises servers.

CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis.

Incorrect options:

Use AWS Lambda to send log data from EC2 instance as well as on-premises servers to CloudWatch Logs

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 centralize the logs from EC2 instances and on-premises servers.

Use CloudWatch Logs for the EC2 instance and CloudTrail for the on-premises servers

Use CloudTrail for the EC2 instance and CloudWatch Logs for the on-premises servers

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. CloudTrail cannot be used to centralize the server logs for EC2 instances or on-premises servers, so both these options are incorrect.

References:

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

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html

Question 45:
Which AWS service will you use if you have to move large volumes of on-premises data to AWS Cloud from a remote location with limited bandwidth?

- **Explanation**

Correct option:

AWS Snowball

AWS Snowball, a part of the AWS Snow Family, is a data migration and edge computing device. If you have large quantities of data you need to migrate into AWS, offline data transfer with AWS Snowball can overcome the challenge of limited bandwidth, and avoid the need to lease additional bandwidth. Snowball moves terabytes of data in about a week. You can use it to move things like databases, backups, archives, healthcare records, analytics datasets, IoT sensor data and media content, especially when network conditions prevent realistic timelines for transferring large amounts of data both into and out of AWS.

Incorrect options:

AWS Virtual Private Network (VPN) - A VPN connection refers to the connection between your Virtual Private Cloud and your on-premises network. By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection, and configuring routing to pass traffic through the connection. VPN aids regular connectivity of AWS and your private om-premises network, it is not a data migration solution.

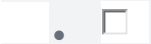
AWS Direct Connect - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you 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. It is not feasible to set up AWS Direct Connect in remote locations.

AWS Transit Gateway - AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. VPC peering across large connections is made possible using Transit Gateway without ending up with a complex VPC peering network. Transit Gateway is not a data migration solution.

Reference:

https://aws.amazon.com/snowball/

Question 46:
AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations for which of the following categories? (Select two)?



Explanation
Correct options:

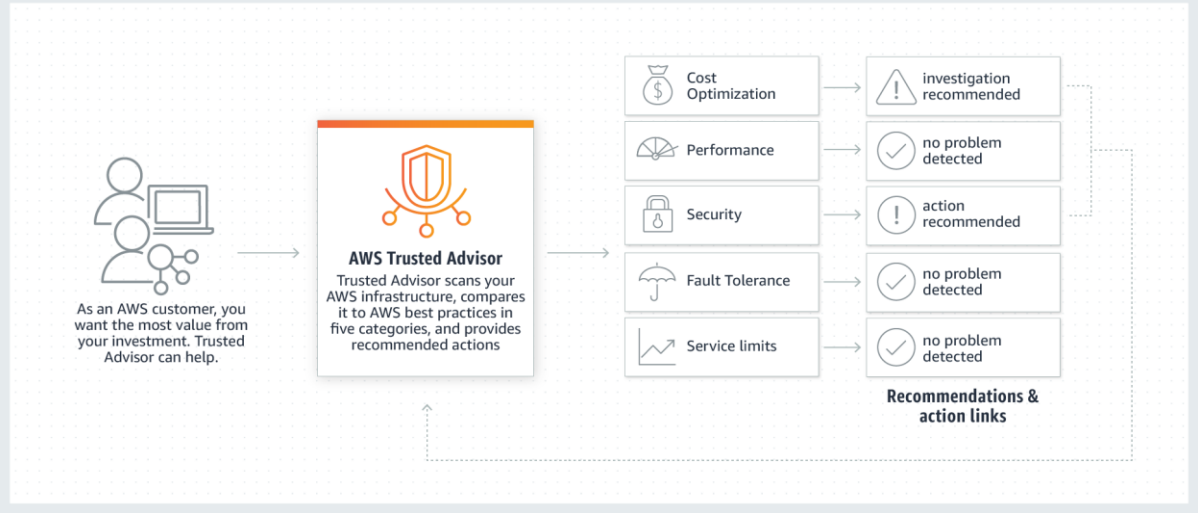
Cost Optimization

Service Limits

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

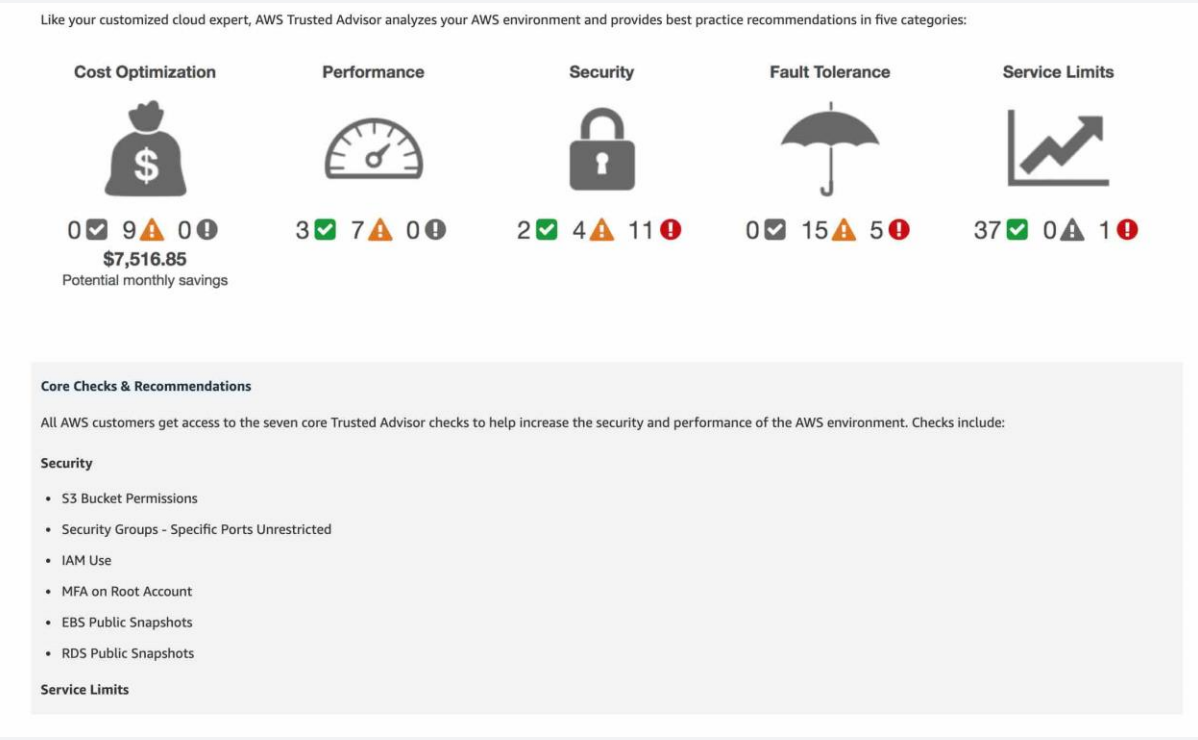
Trusted Advisor on a regular basis help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

How Trusted Advisor Works:



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

AWS Trusted Advisor Recommendations:



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

Incorrect options:

Elasticity

Documentation

Change Management

These three options are made-up and have no importance in the context of AWS Trusted Advisor.

Reference:

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

Question 47: Correct
As a Cloud Practitioner, which S3 storage class would you recommend for data archival?

Explanation
Correct option:

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.

You can further review the use-cases for S3 Glacier:

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

S3 Storage Classes Overview:

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

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

Incorrect options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. It is not suitable for data archival.

S3 Intelligent-Tiering - The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. 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. It is not suitable for data archival.

S3 One Zone-IA - S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ. It is not suitable for data archival.

References:

https://aws.amazon.com/glacier/

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

Question 48:
Which of the following AWS services offer block-level storage? (Select two)

- ☑
- ☐

Explanation

Correct options:

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. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.

Instance Store - An instance store provides temporary block-level storage for your EC2 instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance storage is temporary, data is lost if instance experiences failure or is terminated. EC2 instance store cannot be used for file sharing between instances.

Incorrect options:

EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS file system. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

S3 - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics.

ECS - Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. This is not a storage service and has been added as a distractor.

References:

https://aws.amazon.com/ebs/

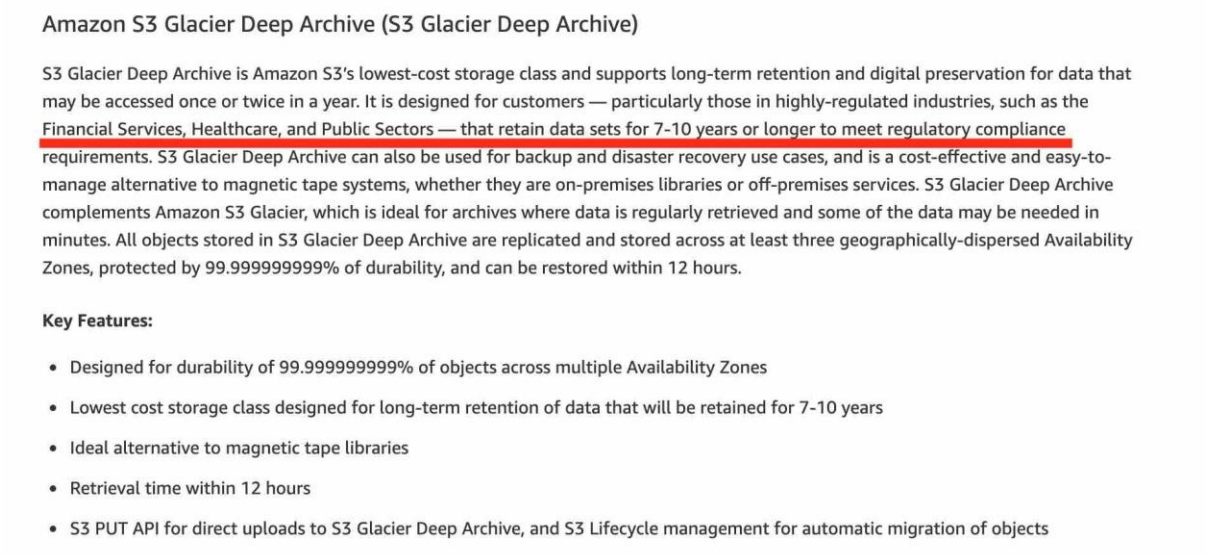
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

Question 49:
A medical device company is looking for a durable and cost-effective way of storing their historic data. Due to compliance requirements, the data must be stored for 10 years. Which AWS Storage solution will you suggest?
Explanation
Correct option:

S3 Glacier Deep Archive

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases. It has a retrieval time (first byte latency) of 12 to 48 hours.

S3 Glacier Deep Archive
Overview:



Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases, and is a cost-effective and easy-to-manage alternative to magnetic tape systems, whether they are on-premises libraries or off-premises services. S3 Glacier Deep Archive complements Amazon S3 Glacier, which is ideal for archives where data is regularly retrieved and some of the data may be needed in minutes. All objects stored in S3 Glacier Deep Archive are replicated and stored across at least three geographically-dispersed Availability Zones, protected by 99.999999999% of durability, and can be restored within 12 hours.

Key Features:

- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Lowest cost storage class designed for long-term retention of data that will be retained for 7-10 years
- Ideal alternative to magnetic tape libraries
- Retrieval time within 12 hours
- S3 PUT API for direct uploads to S3 Glacier Deep Archive, and S3 Lifecycle management for automatic migration of objects

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

Incorrect options:

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. Glacier Deep Archive is a better fit as it is more cost-optimal than Glacier for the given use-case.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways - File, Volume and Tape Gateways). Storage Gateway cannot be used for data archival.

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.

Reference:

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

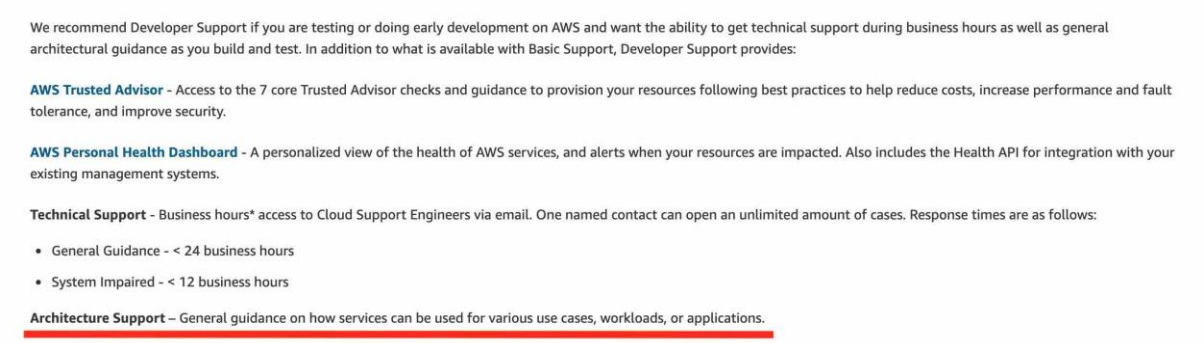
Question 50: Correct
Which AWS Support plan provides general architectural guidance on how services can be used for various use-cases, workloads, or applications?

- **Explanation**

Correct option:

Developer - AWS recommends 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.

Developer Support Plan
Overview:


We recommend Developer Support if you are testing or doing early development on AWS and want the ability to get technical support during business hours as well as general architectural guidance as you build and test. In addition to what is available with Basic Support, Developer Support provides:

AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to help reduce costs, increase performance and fault tolerance, and improve security.

AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted. Also includes the Health API for integration with your existing management systems.

Technical Support - Business hours* access to Cloud Support Engineers via email. One named contact can open an unlimited amount of cases. Response times are as follows:

- General Guidance - < 24 business hours
- System Impaired - < 12 business hours

Architecture Support – General guidance on how services can be used for various use cases, workloads, or applications.

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

Incorrect options:

Enterprise - 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.

Business - AWS recommends 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.

Basic - The basic 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 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted.

Reference:

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

Question 51: Correct
A multi-national company has its business-critical data stored on a fleet of Amazon EC2 instances, in various countries, configured in region-specific compliance rules. To demonstrate compliance, the company needs to submit historical configurations on a regular basis. Which AWS service is best suited for this requirement?

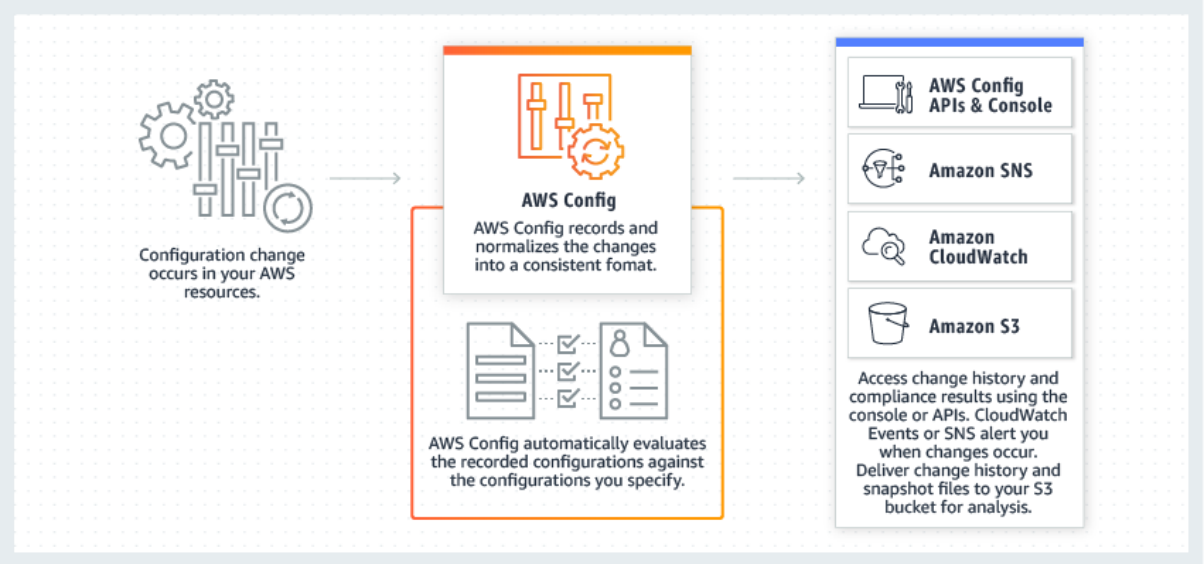
- **Explanation**

Correct option:

AWS Config

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time. AWS Config is designed to help you oversee your application resources in the following scenarios: Resource Administration, Auditing and Compliance, Managing and Troubleshooting Configuration Changes, Security Analysis.

How AWS Config Works:



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

Incorrect options:

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 an added security feature for data privacy and is not the best fit for the current requirement.

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 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.

Config is focused on the configuration of your AWS resources and reports with detailed snapshots on how your resources have changed. Whereas CloudTrail focuses on the events or API calls, that drive those changes. It focuses on the user, application, and activity performed on the system.

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, Amazon VPC Flow Logs, and DNS Logs. Its a threat detection service and not a configuration management and tracking service.

References:

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

https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html

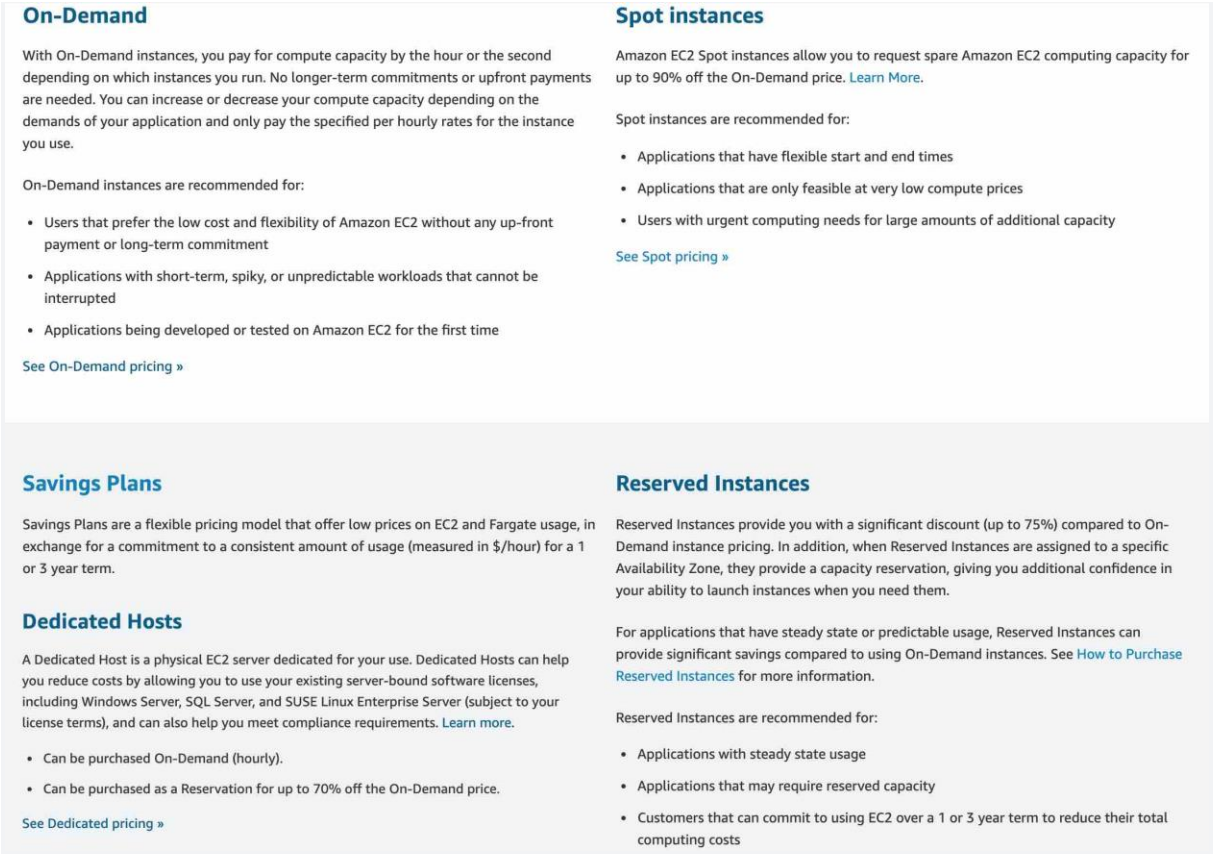
Question 52: **Correct**
A research group wants to provision an EC2 instance for a flexible application that can be interrupted. As a Cloud Practitioner, which of the following would you recommend as the MOST cost-optimal option?

- **Explanation**

Correct option:

Spot Instance - A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts (up to 90%), you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and other flexible tasks that can be interrupted. 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.

EC2 Pricing Options
Overview:



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

Incorrect options:

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. However, On-demand instances are not as cost-effective as spot instances, so this option is not correct.

Reserved Instance - Reserved Instances provide you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. Reserved instances cannot be interrupted. Reserved instances are not as cost-effective as spot instances, so this option is not correct.

Dedicated Host - Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2 so that you get the flexibility and cost-effectiveness of using your 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. They're not cost-efficient compared to spot instances. So this option is not correct.

Reference:

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

Question 53: **Correct**
Which AWS service can be used to automate code deployment to EC2 instances as well as on-premises instances?
Explanation
Correct option:

AWS CodeDeploy

AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone manual operations, and the service scales with your infrastructure so you can easily deploy to one instance or thousands.

Incorrect options:

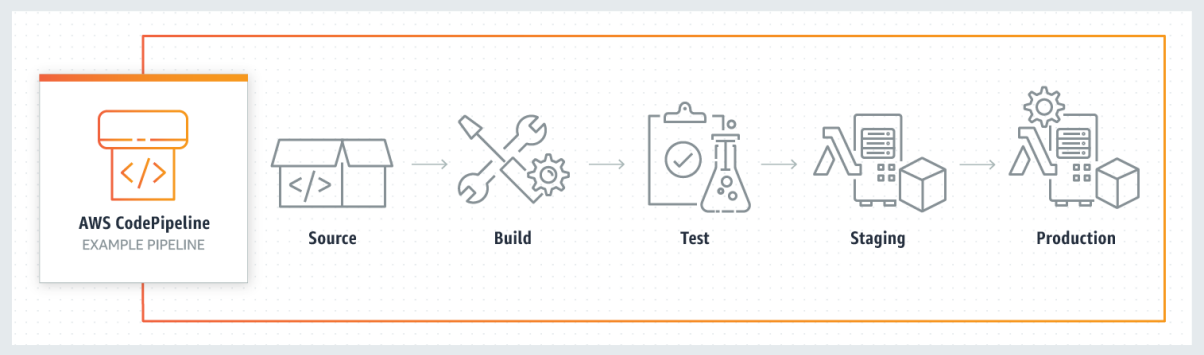
AWS CodeCommit - AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. It cannot be used to automate code deployment.

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. It cannot be used to automate code deployment.

AWS CodePipeline - AWS CodePipeline is a continuous delivery service that enables you to model, visualize, and automate the steps required to release your software. With AWS CodePipeline, you model the full release process for building your code, deploying to pre-production environments, testing your application and releasing it to production.

AWS CodePipeline integrates with AWS services such as AWS CodeCommit, Amazon S3, AWS CodeBuild, AWS CodeDeploy, AWS Elastic Beanstalk, AWS CloudFormation, AWS OpsWorks, Amazon ECS, and AWS Lambda. To further elucidate, CodePipeline cannot by itself deploy the code, it can integrate with CodeDeploy for the actual deployment.

How CodePipeline
Works:



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

Reference:

https://aws.amazon.com/codedeploy/

Question 54: Correct
Once an AWS service has been provisioned, it is expected to work uninterrupted without any network or access issues. In case of any failures, the service should recover quickly. Which pillar of the AWS Well-Architected Framework caters to this ability?

- **Explanation**

Correct option:

Reliability

The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement.

The AWS Well-Architected Framework is based on five pillars — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.

The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross-project requirements, recovery planning, and how we handle change.

Incorrect options:

Operational Excellence - The Operational Excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events.

Security - The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

Performance Efficiency - The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

Reference:

https://wa.aws.amazon.com/wat.pillar.reliability.en.html

Question 55:
An e-commerce company uses AWS Cloud and would like to receive separate invoices for development and production environments. As a Cloud Practioner, which of the following solutions would you recommend for this use-case?

- **Explanation**

Correct option:

"Create separate AWS accounts for development and production environments to receive separate invoices"

Every AWS account provides its own invoice end of the month. You can get separate invoices for development and production environments by setting up separate AWS accounts for each environment.

Incorrect options:

Use AWS Organizations to create separate invoices for development and production environments - 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.

AWS Organizations cannot create separate invoices for development and production environments, rather, AWS Organizations helps you to centrally manage billing.

Tag all resources in the AWS account as either "development" or "production". Then use the tags to create separate invoices - You cannot create separate invoices based on tags.

"Use AWS Cost Explorer to create separate invoices for development and production environments" - 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). AWS Cost Explorer cannot create separate invoices for development and production environments.

Reference:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html

Question 56:
What is the primary benefit of deploying an RDS database in a Read Replica configuration?

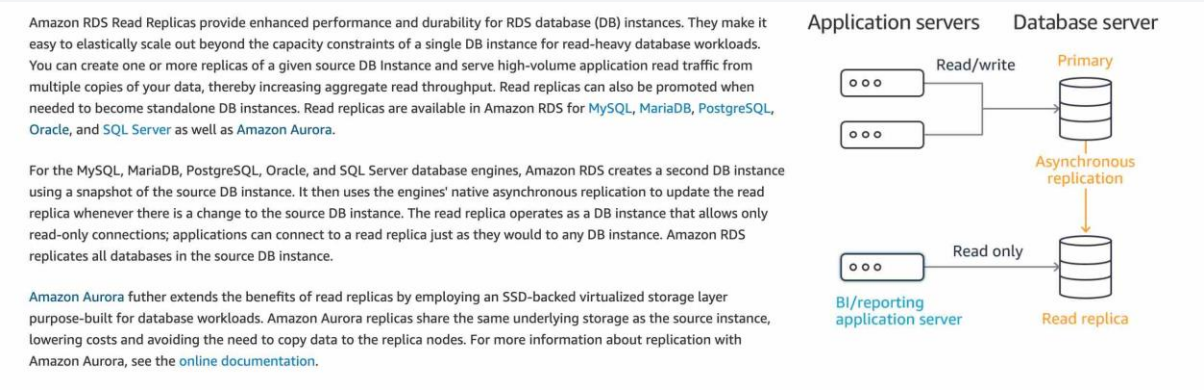
- **Explanation**

Correct option:

Read Replica improves database scalability

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. Read Replicas allow you to create read-only copies that are synchronized with your master database. Read Replicas are used for improved read performance. You can also place your read replica in a different AWS Region closer to your users for better performance. Read Replicas are an example of horizontal scaling of resources.

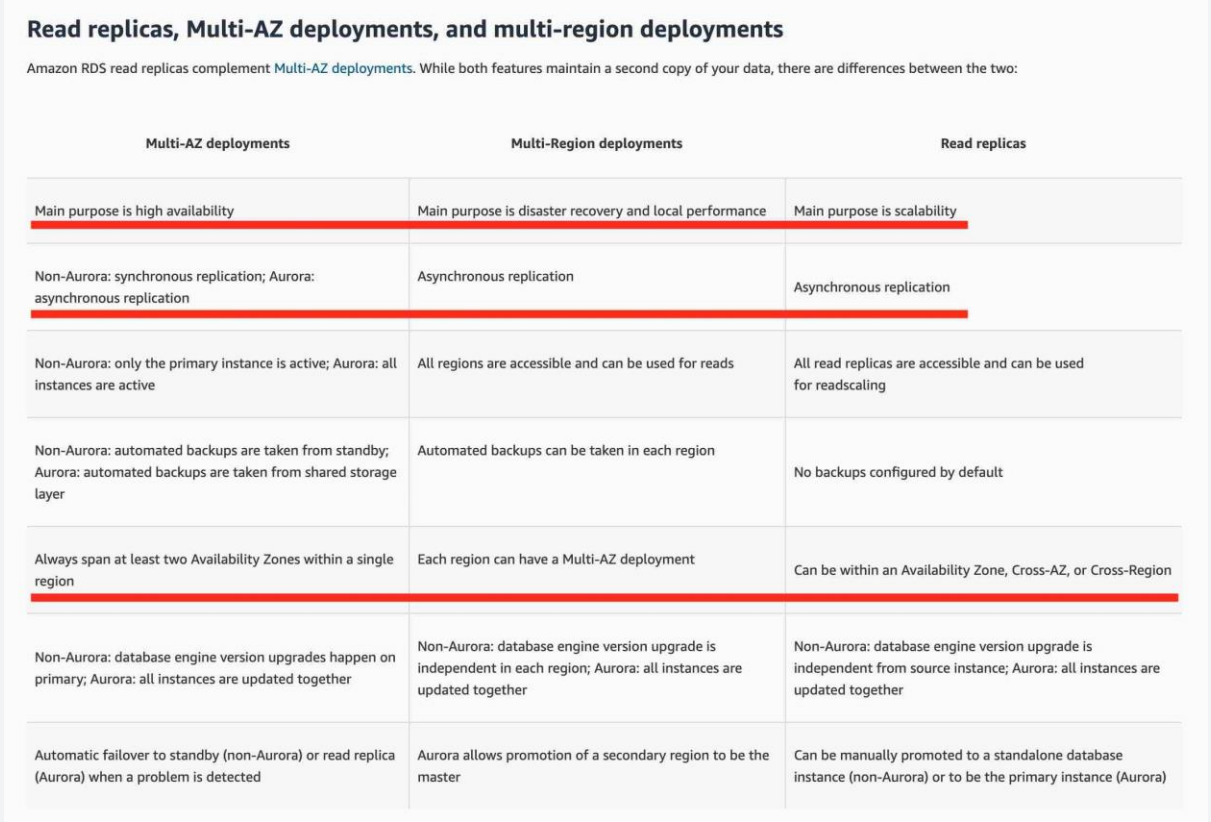
Read Replica
Overview:



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

Exam Alert:

Please review the differences between Multi-AZ, Multi-Region and Read Replica deployments for
RDS:



Read replicas, Multi-AZ deployments, and multi-region deployments

Amazon RDS read replicas complement Multi-AZ deployments. While both features maintain a second copy of your data, there are differences between the two:

Multi-AZ deployments	Multi-Region deployments	Read replicas
Main purpose is high availability	Main purpose is disaster recovery and local performance	Main purpose is scalability
Non-Aurora: synchronous replication; Aurora: asynchronous replication	Asynchronous replication	Asynchronous replication
Non-Aurora: only the primary instance is active; Aurora: all instances are active	All regions are accessible and can be used for reads	All read replicas are accessible and can be used for readscaling
Non-Aurora: automated backups are taken from standby; Aurora: automated backups are taken from shared storage layer	Automated backups can be taken in each region	No backups configured by default
Always span at least two Availability Zones within a single region	Each region can have a Multi-AZ deployment	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Non-Aurora: database engine version upgrades happen on primary; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent in each region; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent from source instance; Aurora: all instances are updated together
Automatic failover to standby (non-Aurora) or read replica (Aurora) when a problem is detected	Aurora allows promotion of a secondary region to be the master	Can be manually promoted to a standalone database instance (non-Aurora) or to be the primary instance (Aurora)

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

Incorrect options:

Read Replica enhances database availability -Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Read Replica cannot enhance database availability.

Read Replica protects the database from a regional failure - You need to use RDS in Multi-Region deployment configuration to protect from a regional failure. Read Replica cannot protect from a regional failure.

Read Replica reduces database usage costs - RDS with Read Replicas increases the database costs compared to the standard deployment. So this option is incorrect.

Reference:

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

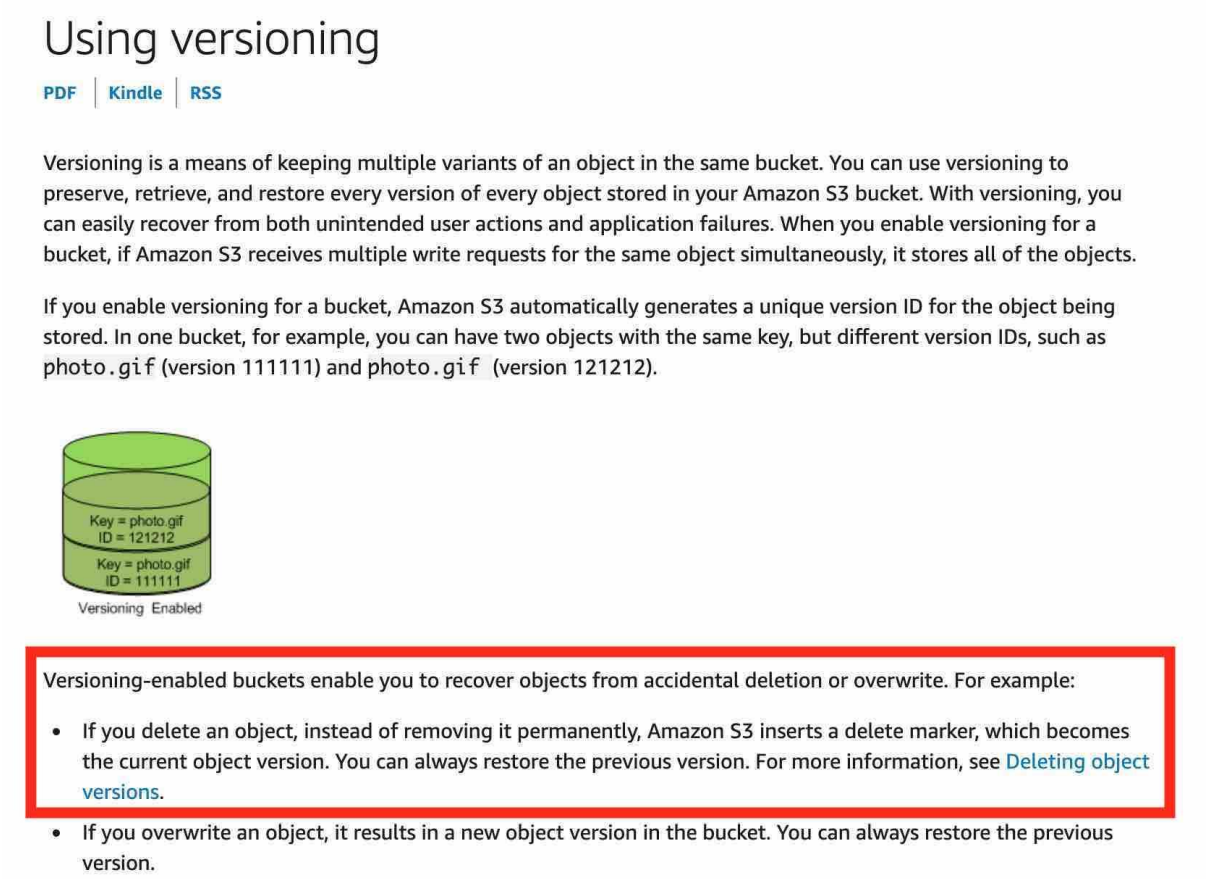
Question 57:
Which of the following is the best way to protect your data from accidental deletion on Amazon S3?
Explanation
Correct option:

S3 Versioning

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

Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. For example: if you delete an object, instead of removing it permanently, Amazon S3 inserts a delete marker, which becomes the current object version.

S3 Versioning
Overview:



via - https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html

Incorrect options:

S3 lifecycle configuration - To manage your S3 objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. With S3 Lifecycle configuration rules, you can tell Amazon S3 to transition objects to less expensive storage classes, or archive or delete them. Lifecycle configuration will do the hard lifting of moving your data into cost-effective storage classes without user intervention. Lifecycle configuration is not meant to protect from accidental deletion of data.

S3 Storage Classes - Amazon S3 offers a range of storage classes designed for different use cases. These include S3 Standard for general-purpose storage of frequently accessed data; S3

Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation. Storage classes are for different storage pattern needs that customers have, and not a data protection mechanism for S3.

S3 Transfer Acceleration - Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path. Transfer Acceleration cannot be used to protect from accidental deletion of data.

Reference:

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

Question 58:
Which of the following are components of an AWS Site-to-Site VPN? (Select two)

- **Explanation**

Correct option:

Virtual Private Gateway

Customer Gateway

AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). VPN Connections are a good solution if you have an immediate need, and have low to modest bandwidth requirements. This connection goes over the public internet. Virtual Private Gateway (or a Transit Gateway) and Customer Gateway are the components of a VPC.

A virtual private gateway is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. A customer gateway is a resource in AWS that provides information to AWS about your Customer gateway device.

Components of an AWS Site-to-Site
VPN:

Components of your Site-to-Site VPN

A Site-to-Site VPN connection offers two VPN tunnels between a virtual private gateway or a transit gateway on the AWS side, and a customer gateway on the remote (on-premises) side.

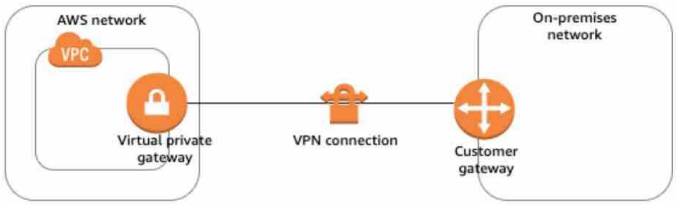
A Site-to-Site VPN connection consists of the following components. For more information about Site-to-Site VPN quotas, see Site-to-Site VPN quotas.

Contents

- Virtual private gateway
- Transit gateway
- Customer gateway
- Customer gateway device

Virtual private gateway

A *virtual private gateway* is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the Site-to-Site VPN connection.



via - https://docs.aws.amazon.com/vpn/latest/s2svpn/how_it_works.html

Incorrect options:

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

NAT Gateway - A NAT Gateway or a NAT Instance can be used in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet. NAT Gateway is managed by AWS but NAT Instance is managed by you.

Internet Gateway - An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It, therefore, imposes no availability risks or bandwidth constraints on your network traffic.

Reference:

https://docs.aws.amazon.com/vpn/latest/s2svpn/how_it_works.html

Question 59:
Which of the following statements are true about Cost Allocation Tags in AWS Billing? (Select two)

- ☐ **Explanation**

Correct options:

For each resource, each tag key must be unique, and each tag key can have only one value

You must activate both AWS generated tags and user-defined tags separately before they can appear in Cost Explorer or on a cost allocation report

A Cost Allocation Tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. For each resource, each tag key must be unique, and each tag key can have only one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level.

AWS provides two types of cost allocation tags, an AWS generated tags and user-defined tags. AWS defines, creates, and applies the AWS generated tags for you, and you define, create, and apply user-defined tags. You must activate both types of tags separately before they can appear in Cost Explorer or on a cost allocation report.

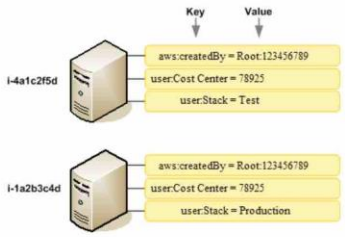
AWS Cost Allocation Tags
Overview:

Using Cost Allocation Tags

PDF | Kindle | RSS

A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a *key* and a *value*. For each resource, each tag key must be unique, and each tag key can have only one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs. AWS provides two types of cost allocation tags, an *AWS generated tags* and *user-defined tags*. AWS defines, creates, and applies the AWS generated tags for you, and you define, create, and apply user-defined tags. You must activate both types of tags separately before they can appear in Cost Explorer or on a cost allocation report.

The following diagram illustrates the concept. In the example, you've assigned and activated tags on two Amazon EC2 instances, one tag called Cost Center and another tag called Stack. Each of the tags has an associated value. You also activated the AWS generated tags, `createdBy` before creating these resources. The `createdBy` tag tracks who created a resource. The user-defined tags use the `user` prefix, and the AWS generated tag uses the `aws:` prefix.



After you or AWS applies tags to your AWS resources (such as Amazon EC2 instances or Amazon S3 buckets) and you activate the tags in the Billing and Cost Management console, AWS generates a cost allocation report as a comma-separated value (CSV file) with your usage and costs grouped by your active tags. You can apply tags that represent business categories (such as cost centers, application names, or owners) to organize your costs across multiple services.

The cost allocation report includes all of your AWS costs for each billing period. The report includes both tagged and untagged resources, so that you can clearly organize the charges for resources. For example, if you tag resources with an application name, you can track the total cost of a single application that runs on those resources. The following screenshot shows a partial report with columns for each tag.

Total Cost	user:Owner	user:Stack	user:Cost Center	user:Application
0.95	DbAdmin	Test	80432	Widget2
0.01	DbAdmin	Test	80432	Widget2
3.84	DbAdmin	Prod	80432	Widget2
6.00	DbAdmin	Test	78925	Widget1
234.63	SysEng	Prod	78925	Widget1
0.73	DbAdmin	Test	78925	Widget1
0.00	DbAdmin	Prod	80432	Portal

via - https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html

Incorrect options:

Tags helps in organize resources and are a mandatory configuration item to run reports - Tags definitely help organize resources as per an organization's requirement; they are not mandatory though.

For each resource, each tag key must be unique, but can have multiple values - For each resource, each tag key must be unique, and each tag key can have only one value.

Only user-defined tags need to be activated before they can appear in Cost Explorer or on a cost allocation report - As explained above, both kinds of tags (user-defined and AWS generated) need to be activated separately before they can appear in report generation.

Reference:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html

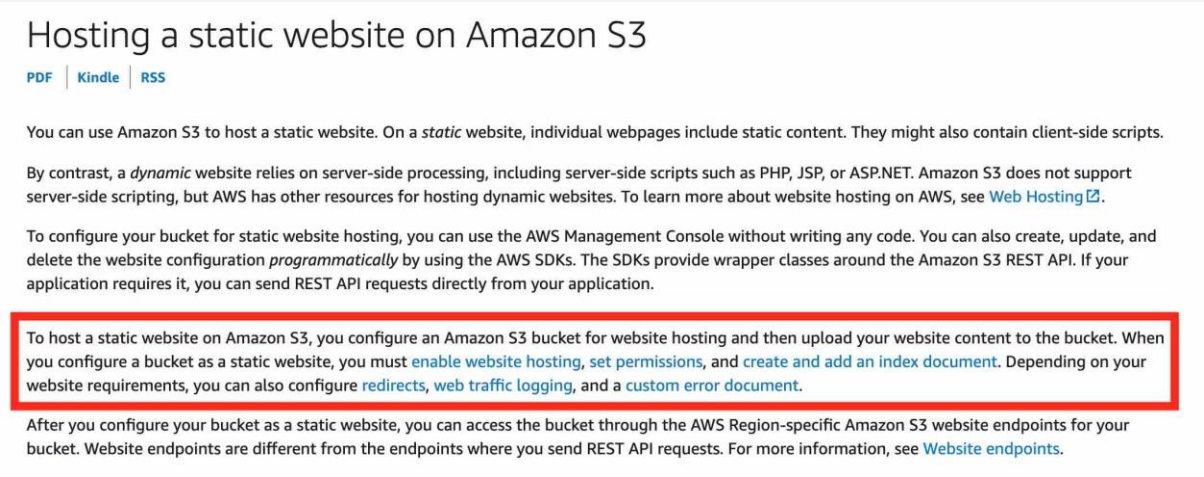
Question 60:
An IT company has deployed a static website on S3, but the website is still inaccessible. As a Cloud Practioner, which of the following solutions would you suggest to address this issue?

Explanation
Correct options:

Fix the S3 bucket policy

To host a static website on Amazon S3, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket. When you configure a bucket as a static website, you must enable website hosting, set permissions, and create and add an index document.

Hosting a static website on Amazon S3:


Hosting a static website on Amazon S3

PDF | Kindle | RSS

You can use Amazon S3 to host a static website. On a *static* website, individual webpages include static content. They might also contain client-side scripts.

By contrast, a *dynamic* website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting, but AWS has other resources for hosting dynamic websites. To learn more about website hosting on AWS, see Web Hosting.

To configure your bucket for static website hosting, you can use the AWS Management Console without writing any code. You can also create, update, and delete the website configuration *programmatically* by using the AWS SDKs. The SDKs provide wrapper classes around the Amazon S3 REST API. If your application requires it, you can send REST API requests directly from your application.

To host a static website on Amazon S3, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket. When you configure a bucket as a static website, you must enable website hosting, set permissions, and create and add an index document. Depending on your website requirements, you can also configure redirects, web traffic logging, and a custom error document.

After you configure your bucket as a static website, you can access the bucket through the AWS Region-specific Amazon S3 website endpoints for your bucket. Website endpoints are different from the endpoints where you send REST API requests. For more information, see Website endpoints.

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

If you want to configure an existing bucket as a static website that has public access, you must edit block public access settings for that bucket. You may also have to edit your account-level block public access settings. Amazon S3 applies the most restrictive combination of the bucket-level and account-level block public access settings.

Here is how you can edit Public Access settings for S3 buckets: via
- https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteAccessPermissionsReqd.html

Incorrect options:

Disable S3 encryption

Enable S3 versioning

Enable S3 replication

Disabling S3 encryption, enabling S3 versioning or replication have no bearing on deploying a static website on S3, so these options are not correct.

References:

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

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

Question 61:
A research lab wants to optimize the caching capabilities for its scientific computations application running on EC2 instances. Which EC2 storage option is best suited for this use-case?

- **Explanation**

Correct option:

Amazon EC2 Instance Store

An Instance Store provides temporary block-level storage for your EC2 instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance storage is temporary, data is lost if instance experiences failure or is terminated.

Instance Store
Overview:

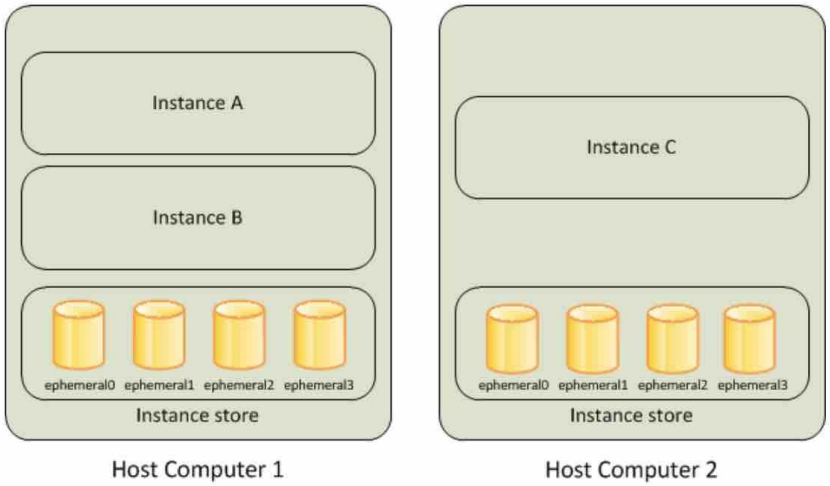
Amazon EC2 Instance Store

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 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. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS. EBS is not a good fit for caching information on EC2 instances.

Amazon EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS file system. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies. EFS is not a good fit for caching information on EC2 instances.

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 a good fit for caching information on EC2 instances.

Reference:

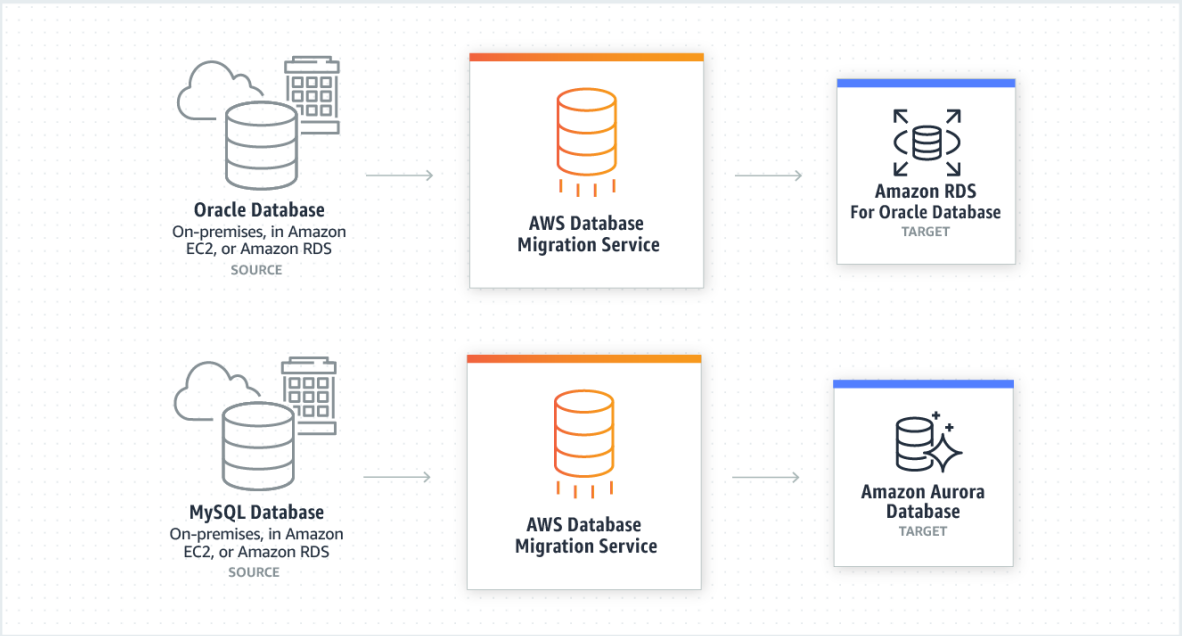
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

Question 62:
Which of the following AWS services specialize in data migration from on-premises to AWS Cloud? (Select two)
Explanation
Correct options:

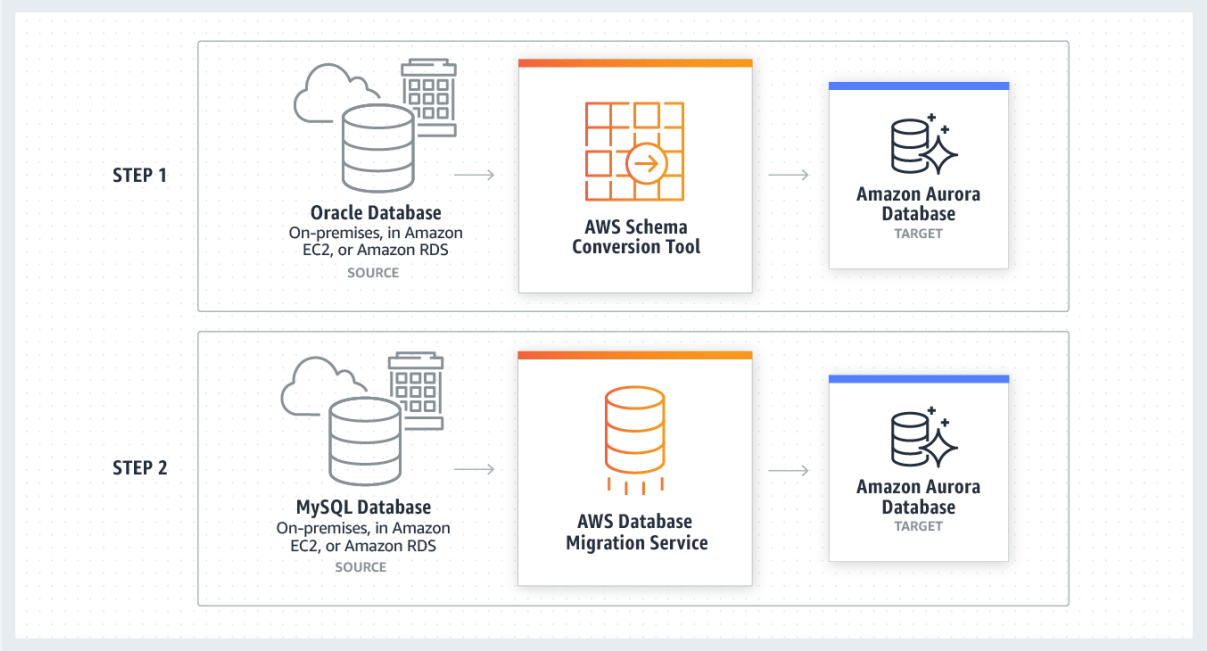
Snowball - AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS services using storage devices designed to be secure for physical transport.

Database Migration Service - AWS Database Migration Service helps you migrate databases from on-premises 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 can migrate your data to and from the most widely used commercial and open-source databases.

You can do both homogeneous and heterogeneous database migration using Database Migration
Service:



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



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

Incorrect options:

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. Site to Site VPN is a connectivity service and it does not specialize in data migration.

Direct Connect - AWS Direct Connect creates a dedicated private connection from a remote network to your VPC. This is a private connection and does not use the public internet. Takes at least a month to establish this connection. Direct Connect is a connectivity service and it does not specialize in data migration.

Transit Gateway - AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. As you expand globally, inter-Region peering connects AWS Transit Gateways using the AWS global network. Your data is automatically encrypted and never travels over the public internet. Transit Gateway is a connectivity service and it does not specialize in data migration.

References:

https://aws.amazon.com/getting-started/projects/migrate-petabyte-scale-data/services-costs/

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

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

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

Question 63: **Correct**

Which of the following AWS entities provides the information required to launch an EC2 instance?
Explanation
Correct option:

AMI

An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance.

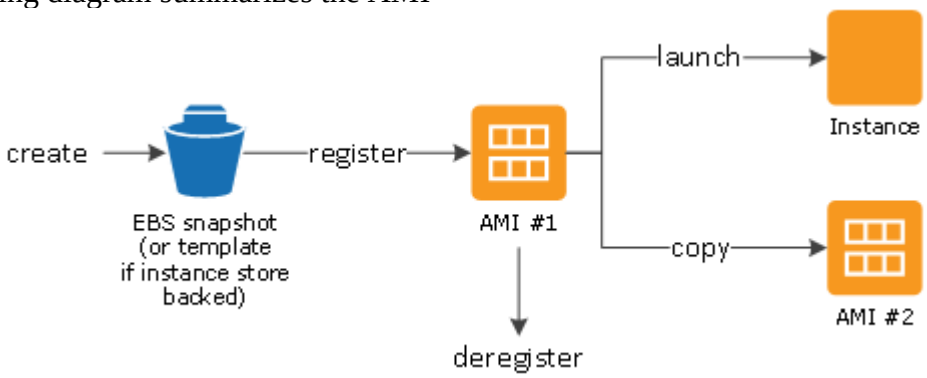
An AMI includes the following:

One or more EBS snapshots, or, for instance-store-backed AMIs, a template for the root volume of the instance (for example, an operating system, an application server, and applications).

Launch permissions that control which AWS accounts can use the AMI to launch instances.

A block device mapping that specifies the volumes to attach to the instance when it's launched.

The following diagram summarizes the AMI lifecycle:



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

Incorrect options:

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

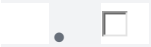
EFS - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove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

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.

Reference:

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

Question 64:
Which of the following are recommended best practices for AWS IAM service? (Select two)



Explanation
Correct option:

Enable MFA for all users - AWS recommends that you require multi-factor authentication (MFA) for all users in your account. With MFA, users have a device that generates a response to an authentication challenge. Both the user's credentials and the device-generated response are required to complete the sign-in process.

Rotate credentials regularly - AWS recommends that you change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a password policy to your account to require all your IAM users to rotate their passwords.

AWS IAM security best
practices:

Security Best Practices in IAM

PDF | Kindle | RSS

To help secure your AWS resources, follow these recommendations for the AWS Identity and Access Management (IAM) service.

Topics

- Lock Away Your AWS Account Root User Access Keys
- Create Individual IAM Users
- Use Groups to Assign Permissions to IAM Users
- Grant Least Privilege
- Get Started Using Permissions with AWS Managed Policies
- Use Customer Managed Policies Instead of Inline Policies
- Use Access Levels to Review IAM Permissions
- Configure a Strong Password Policy for Your Users
- Enable MFA
- Use Roles for Applications That Run on Amazon EC2 Instances
- Use Roles to Delegate Permissions
- Do Not Share Access Keys
- Rotate Credentials Regularly
- Remove Unnecessary Credentials
- Use Policy Conditions for Extra Security
- Monitor Activity in Your AWS Account

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

Incorrect options: **Create a minimum number of accounts and share these account credentials among employees** - AWS recommends that user account credentials should not be shared between users.

Grant maximum privileges to avoid assigning privileges again - AWS recommends granting the least privileges required to complete a certain job and avoid giving excessive privileges which can be misused.

Share AWS account root user access keys with other administrators - The access key for your AWS account root user gives full access to all your resources for all AWS services, including your billing information. You cannot reduce the permissions associated with your AWS account root user access key. You should never share these access keys with any other users, not even the administrators.

Reference:

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

Question 65:
AWS Lambda pricing is based on which of the following criteria? (Select two)

- ☐ **Explanation**

Correct options:

Number of requests for the lambda function

The time it takes for the lambda function to execute

AWS Lambda lets you run code without provisioning or managing servers. 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.

With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the duration, the time it takes for your code to execute. Lambda counts a request each time it starts executing in response to an event notification or invoke call, including test invokes from the console. Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms.

Incorrect options:

The language runtime of the lambda function - Lambda supports many programming language runtimes such as NodeJS, Python, Go, C# etc. The pricing for a lambda function is not dependent on the language runtime of the lambda function.

The number of lines of code for the lambda function - The pricing for a lambda function is not dependent on the number of lines of code for the lambda function.

The size of the deployment package for the lambda function - The pricing for a lambda function is not dependent on the size of the deployment package for the lambda function.

Reference:

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