Question 1:

Which of the following types are free under the Amazon S3 pricing model? (Select two)

- 

Explanation
Correct options:

Data transferred in from the internet

Data transferred out to an Amazon Elastic Compute Cloud (Amazon EC2) instance, when the instance is in the same AWS Region as the S3 bucket

There are four cost components to consider for S3 pricing – storage pricing; request and data retrieval pricing; data transfer and transfer acceleration pricing; and data management features pricing. Under "Data Transfer", You pay for all bandwidth into and out of Amazon S3, except for the following: (1) Data transferred in from the internet, (2) Data transferred out to an Amazon Elastic Compute Cloud (Amazon EC2) instance, when the instance is in the same AWS Region as the S3 bucket, (3) Data transferred out to Amazon CloudFront (CloudFront).

Incorrect options:

Data transferred out to an Amazon Elastic Compute Cloud (Amazon EC2) instance in any AWS Region - This is incorrect. Data transfer charges apply when the instance is not in the same AWS Region as the S3 bucket.

Data storage fee for objects stored in S3 Standard - S3 Standard charges a storage fee for objects.

Data storage fee for objects stored in S3 Glacier - S3 Glacier charges a storage fee for objects.

Reference:

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

Question 2:

Which of the following is correct regarding the AWS RDS service?

- 

Explanation
Correct option:

You can use Read Replicas for improved read performance and Multi-AZ for Disaster Recovery

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

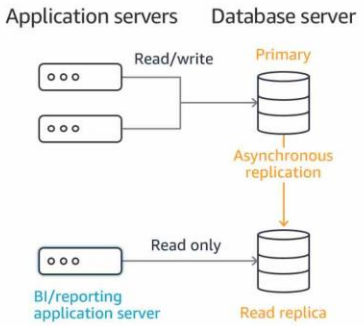
performance. You can also place your read replica in a different AWS Region closer to your users for better performance. Read Replicas are an example of horizontal scaling of resources.

Read Replica
Overview:

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.

For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Amazon Aurora futher extends the benefits of read replicas by employing an SSD-backed virtualized storage layer purpose-built for database workloads. Amazon Aurora replicas share the same underlying storage as the source instance, lowering costs and avoiding the need to copy data to the replica nodes. For more information about replication with Amazon Aurora, see the online documentation.

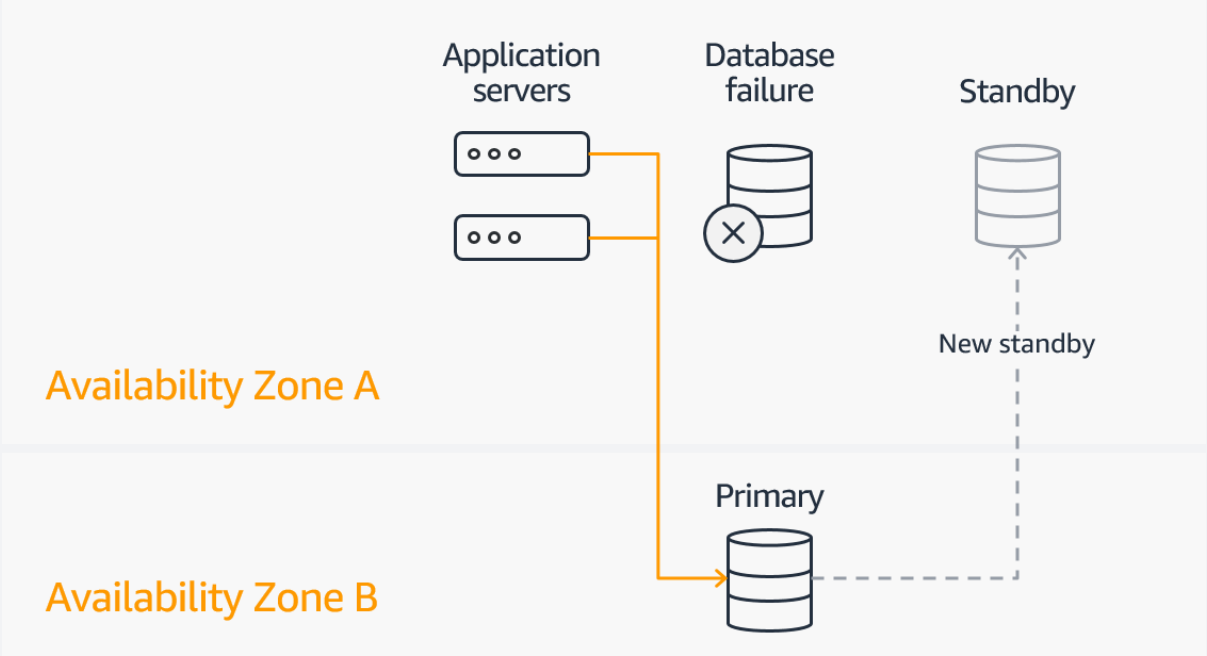


via - https://aws.amazon.com/rds/features/multi-az/

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).

In case of an infrastructure failure (such as a disaster), Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

How Multi-AZ
Works:



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

Incorrect options:

You can use both Read Replicas and Multi-AZ for Disaster Recovery

You can use both Read Replicas and Multi-AZ for improved read performance

You can use Read Replicas for Disaster Recovery and Multi-AZ for improved read performance

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

Reference:

Question 3:

The DevOps team at an IT company wants to centrally manage its servers on AWS Cloud as well as on-premise data center so that it can run commands, configure and patch servers at scale. As a Cloud Practitioner, which AWS service would you recommend for this use-case?

- OpsWorks
- Systems Manager **(Correct)**
- Config
- CloudFormation

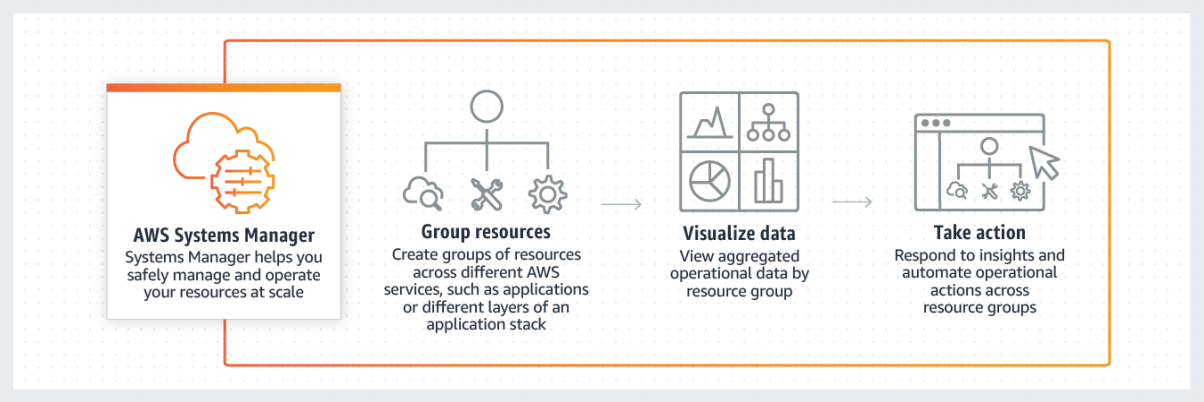
Explanation
Correct option:

Systems Manager

AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks such as running commands, managing patches, and configuring servers across AWS Cloud as well as on-premises infrastructure.

AWS Systems Manager offers utilities for running commands, patch-management and

configuration compliance: via - https://aws.amazon.com/systems-manager/faq/



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

Incorrect options:

OpsWorks - AWS OpsWorks is a configuration management service that provides managed instances of **Chef and Puppet**. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed and managed across your Amazon EC2 instances or on-premises compute environments. You cannot use OpsWorks for running commands or managing patches on servers.

CloudFormation - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. You cannot use CloudFormation for running commands or managing patches on servers.

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. **You cannot use Config for running commands or managing patches on servers.**

References:

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

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

Question 4: Correct
Which AWS service would you use to create a logically isolated section of the AWS Cloud where you can launch AWS resources in your virtual network?

- Network Access Control List (NACL)
- Virtual Private Cloud (VPC) **(Correct)**
- Subnet
- Virtual Private Network (VPN)

Explanation
Correct option:

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. You can easily customize the network configuration of your Amazon VPC using public and private subnets.

Incorrect options:

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. You cannot use VPN to create a logically isolated section of the AWS Cloud.

Subnet - A subnet is a range of IP addresses within your VPC. A subnet is not an AWS service, so this option is ruled out.

Network Access Control List (NACL) - 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. A NACL is not an AWS service, so this option is ruled out.

Reference:

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

Question 5: Incorrect

Which of the following statements are CORRECT regarding AWS Global Accelerator? (Select two)

- ☐ Global Accelerator is a good fit for non-HTTP use cases
  (Correct)
- ☐ Global Accelerator can be used to host static websites
- ☑ Global Accelerator uses the AWS global network and its edge locations. But the edge locations used by Global Accelerator are different from Amazon CloudFront edge locations
  (Incorrect)
- ☑ Global Accelerator provides static IP addresses that act as a fixed entry point to your applications
  (Correct)
- ☐ Global Accelerator cannot be configured with an Elastic Load Balancer (ELB)

Explanation
Correct options:

AWS Global Accelerator is a networking service that helps you improve the availability and performance of the applications that you offer to your global users. Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions.

How Global Accelerator Works:

via - https://aws.amazon.com/global-accelerator/

Global Accelerator is a good fit for non-HTTP use cases - Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

Global Accelerator provides static IP addresses that act as a fixed entry point to your applications - It provides static IP addresses that provide a fixed entry point to your applications and eliminate the complexity of managing specific IP addresses for different AWS Regions and Availability Zones.

Incorrect options:

Global Accelerator uses the AWS global network and its edge locations. But the edge locations used by Global Accelerator are different from Amazon CloudFront edge locations - AWS Global Accelerator and Amazon CloudFront use the same edge locations.

Global Accelerator cannot be configured with an Elastic Load Balancer (ELB) - A regional ELB load balancer is an ideal target for AWS Global Accelerator. AWS Global Accelerator complements ELB by extending these capabilities beyond a single AWS Region, allowing you to provide a global interface for your applications in any number of Regions.

Global Accelerator can be used to host static websites - Amazon S3 can host static websites. So this option is incorrect.

Reference:

https://aws.amazon.com/global-accelerator/

Question 6: Correct
Which of the following entities can be used to connect to an EC2 server from a Mac OS, Windows or Linux based computer via a browser-based client?

- Putty
- SSH
- AWS Direct Connect
- EC2 Instance Connect **(Correct)**

Explanation
Correct option:

EC2 Instance Connect

Amazon EC2 Instance Connect provides a simple and secure way to connect to your instances using Secure Shell (SSH). With EC2 Instance Connect, you use AWS Identity and Access Management (IAM) policies and principals to control SSH access to your instances, removing the need to share and manage SSH keys. All connection requests using EC2 Instance Connect are logged to AWS CloudTrail so that you can audit connection requests.

You can use Instance Connect to connect to your Linux instances using a browser-based client, the Amazon EC2 Instance Connect CLI, or the SSH client of your choice. EC2 Instance Connect can be used to connect to an EC2 instance from a Mac OS, Windows or Linux based computer.

Incorrect options:

SSH - SSH can be used from a Mac OS, Windows or Linux based computer, but it's not a browser-based client.

Putty - Putty can be used only from Windows based computers.

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. Direct Connect cannot be used to connect to an EC2 instance from a Mac OS, Windows or Linux based computer.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html

Question 7: Correct
Which of the following AWS services offer LifeCycle Management for cost-optimal storage?

- Amazon Instance Store
- Amazon EBS
- AWS Storage Gateway
- Amazon S3 **(Correct)**

Explanation
Correct options:

Amazon S3

You can manage your objects on S3 so that they are stored cost-effectively throughout their lifecycle by configuring their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects.

There are two types of actions:

Transition actions — Define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

Expiration actions — Define when objects expire. Amazon S3 deletes expired objects on your behalf.

Incorrect options:

Amazon 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 does not offer Lifecycle Management or Infrequent Access storage class.

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. It does not offer Lifecycle Management or Infrequent Access storage class.

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 does not offer Lifecycle Management or Infrequent Access storage class.

References:

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

Question 8: Correct
Which of the following are benefits of the AWS Web Application Firewall (WAF)? (Select two)

- [ ] WAF offers dedicated support from the DDoS Response Team (DRT) and advanced reporting
- [x] WAF can block all requests except the ones that you specify **(Correct)**
- [ ] WAF offers protection against all known infrastructure (Layer 3 and 4) attacks
- [ ]

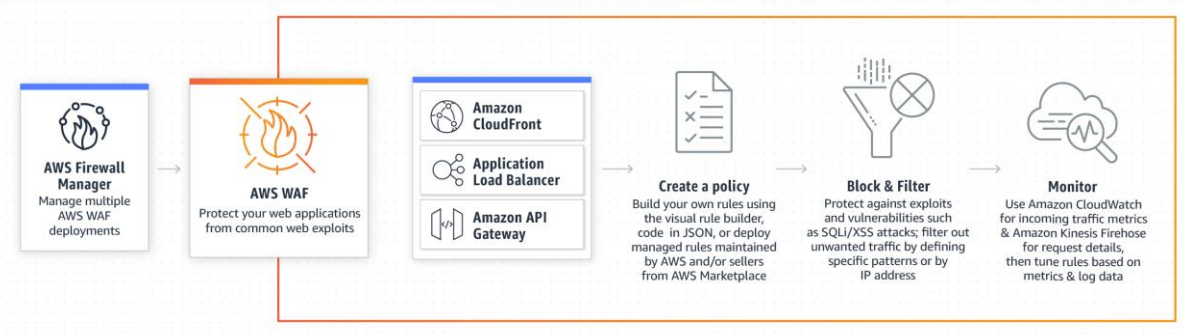
AWS WAF lets you monitor the HTTP and HTTPS requests that are forwarded to Amazon Route 53

- ☑ WAF can check for the presence of SQL code that is likely to be malicious (known as SQL injection)
  (Correct)

Explanation
Correct options:

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns such as SQL injection or cross-site scripting. You can also use rate-based rules to mitigate the Web layer DDoS attack.

How WAF Works:



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

WAF can block all requests except the ones that you specify - WAF can block all requests except the ones that you specify. This is useful when you want to serve content for a restricted website whose users are readily identifiable by properties in web requests, such as the IP addresses that they use to browse to the website.

WAF can check for the presence of SQL code that is likely to be malicious (known as SQL injection) - WAF offers additional protection against web attacks using conditions that you specify. You can define conditions by using characteristics of web requests such as - IP addresses that requests originate from, presence of a script that is likely to be malicious (known as cross-site scripting), presence of SQL code that is likely to be malicious (known as SQL injection) and many more.

Incorrect options:

WAF offers protection against all known infrastructure (Layer 3 and 4) attacks - WAF lets you monitor the HTTP and HTTPS requests to your application, it only works at the application layer (layer 7).

WAF offers dedicated support from the DDoS Response Team (DRT) and advanced reporting - As AWS Shield Advanced customer can contact a 24x7 DDoS response team (DRT) for assistance during a DDoS attack, it is a feature of Shield Advanced, and not of WAF.

AWS WAF lets you monitor the HTTP and HTTPS requests that are forwarded to Amazon Route 53 - AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. It does not cover Amazon Route 53, which is a Domain Name System (DNS) web service.

Reference:

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

Question 9: **Correct**
Which of the following AWS entities lists all users in your account and the status of their various account aspects such as passwords, access keys, and MFA devices?

- AWS Trusted Advisor
- Amazon Inspector
- AWS Cost and Usage Reports
- Credential Reports **(Correct)**

Explanation
Correct option:

Credential Reports

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can use credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password and access key rotation. You can provide the report to an external auditor, or grant permissions to an auditor so that he or she can download the report directly.

Incorrect options:

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 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 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.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

Question 10: Correct
Reserved Instance pricing is available for which of the following AWS services? (Select two)

- [x] Amazon Elastic Compute Cloud (Amazon EC2) **(Correct)**
- [x] Amazon Relational Database Service (Amazon RDS) **(Correct)**
- [ ] Amazon CloudFront
- [ ] Amazon Simple Storage Service (Amazon S3)
- [ ] AWS Identity & Access Management (IAM)

Explanation
Correct options:

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Relational Database Service (Amazon RDS)

A Reserved Instance is a reservation that provides a discounted hourly rate in exchange for an upfront fee and term contract. Services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) use this approach to sell reserved capacity for hourly use of Reserved Instances. It is not a virtual machine. It is a commitment to pay in advance for specific Amazon EC2 or Amazon RDS instances.

Incorrect options:

Amazon CloudFront - Amazon CloudFront is a content delivery network (CDN) service. CloudFront does not offer "Reserved Capacity" pricing.

Amazon Simple Storage Service (Amazon S3) - Amazon S3 infrastructure is managed by AWS. So, Reserved Instance does not make sense here. But, S3 offers volume discounts for its storage classes.

AWS Identity & 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. This is a free service to every AWS customer.

Reference:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/con-bill-blended-rates.html

Question 11: Correct
Which entity ensures that your application on Amazon EC2 always has the right amount of capacity to handle the current traffic demand?

- Auto Scaling **(Correct)**
- Multi AZ deployment
- Application Load Balancer
- Network Load Balancer

Explanation
Correct option:

Auto Scaling

Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size.

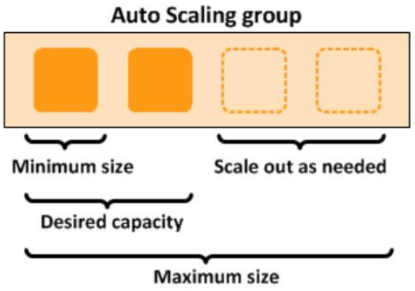
EC2 Auto Scaling
Overview:

What Is Amazon EC2 Auto Scaling?

PDF | Kindle | RSS

Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called *Auto Scaling groups*. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size. If you specify the desired capacity, either when you create the group or at any time thereafter, Amazon EC2 Auto Scaling ensures that your group has this many instances. If you specify scaling policies, then Amazon EC2 Auto Scaling can launch or terminate instances as demand on your application increases or decreases.

For example, the following Auto Scaling group has a minimum size of one instance, a desired capacity of two instances, and a maximum size of four instances. The scaling policies that you define adjust the number of instances, within your minimum and maximum number of instances, based on the criteria that you specify.



via - https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

Incorrect options:

Multi AZ deployment - With Availability Zones, you can design and operate applications and databases that automatically failover between zones without interruption. Multi AZ deployment of EC2 instances provided high availability, it does not help in scaling resources.

Network Load Balancer - Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required. It distributes traffic, does not scale resources.

Application Load Balancer - An Application Load Balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. It distributes traffic, does not scale resources.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

Question 12: Correct

Which of the following AWS storage services can be directly used with on-premises systems?

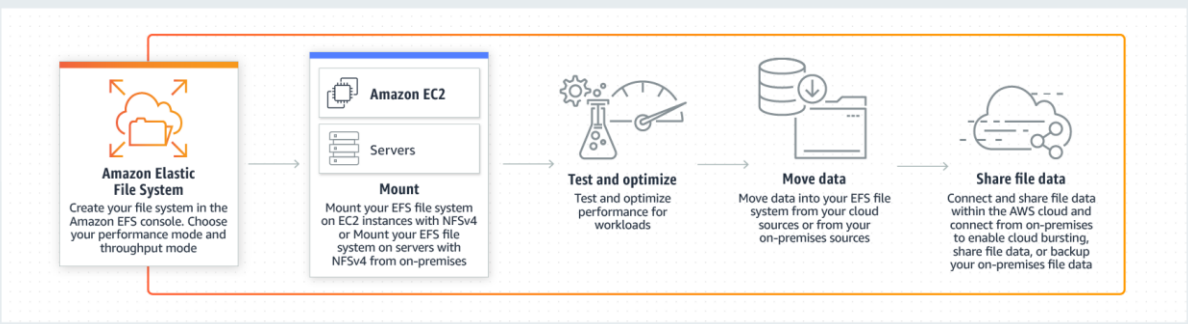
- Amazon Elastic File System (Amazon EFS) **(Correct)**
- Amazon Elastic Block Store (EBS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon EC2 Instance Store

Explanation
Correct option: **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.

To access EFS file systems from on-premises, you must have an AWS Direct Connect or AWS VPN connection between your on-premises datacenter and your Amazon VPC. You mount an EFS file system on your on-premises Linux server using the standard Linux mount command for mounting a file system

How EFS Works:



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

Incorrect options:

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

Amazon EC2 Instance Store - An instance store provides temporary block-level storage for your Amazon EC2 instance. This storage is located on disks that are physically attached to the host computer. It is not possible to use this storage from on-premises systems.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 can be accessed from on-premises only via AWS Storage Gateway. It is not possible to access S3 directly from on-premises systems.

Reference:

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

Question 13: Correct
Which of the following is the MOST cost-effective EC2 instance purchasing option for short-term, spiky and critical workloads on AWS Cloud?

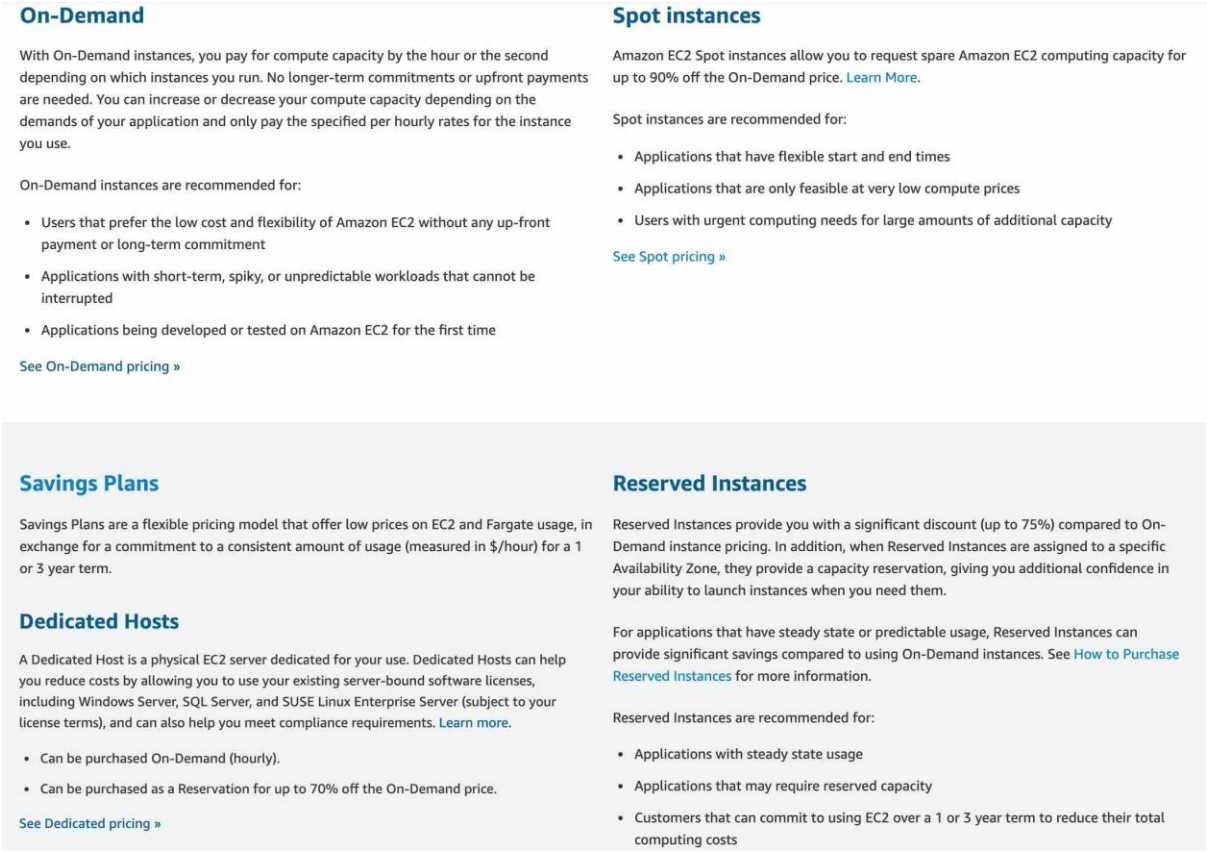
- On-Demand Instance **(Correct)**
- Reserved Instance
- Dedicated Host
- Spot Instance

Explanation
Correct option:

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. There is no need for a long-term purchasing commitment. The price per second for running an On-Demand Instance is fixed. On-demand instances cannot be interrupted. Therefore On-Demand instances are the best fit for short-term, spiky and critical workloads.

EC2 Pricing Options
Overview:



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

Incorrect options:

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.

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 the right choice for short-term workloads.

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 On-Demand instances. So this option is not correct.

Reference:

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

Question 14: Correct
Which AWS service will you use to provision the same AWS infrastructure across multiple AWS accounts and regions?

- AWS CodeDeploy
- AWS Systems Manager
- AWS OpsWorks
- AWS CloudFormation **(Correct)**

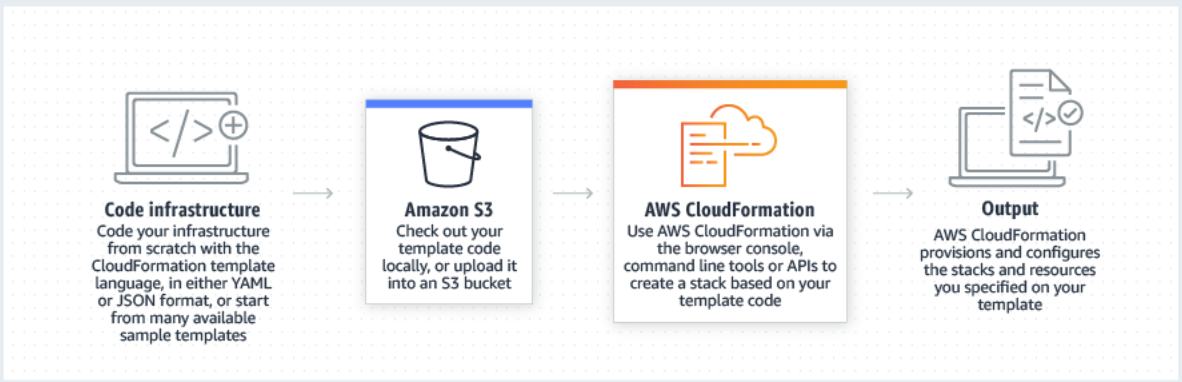
Explanation
Correct option:

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. A stack is a collection of AWS resources that you can manage as a single unit. In other words, you can create, update, or delete a collection of resources by creating, updating, or deleting stacks.

AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation. Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified regions.

How CloudFormation Works:



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

Incorrect options:

AWS CodeDeploy - AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during application deployment, and handles the complexity of updating your applications. You cannot use this service to provision AWS infrastructure.

AWS OpsWorks - AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed and managed across your Amazon EC2 instances or on-premises compute environments. You cannot use OpsWorks for running commands or managing patches on servers. You cannot use this service to provision AWS infrastructure.

AWS Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. You cannot use this service to provision AWS infrastructure.

Reference:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/what-is-cfnstacksets.html

Question 15: **Correct**
A media company uploads its media (audio and video) files to a centralized S3 bucket from geographically dispersed locations. Which of the following solutions can the company use to optimize transfer speeds?

- S3 Transfer Acceleration **(Correct)**
- Amazon CloudFront
- AWS Global Accelerator
- AWS Direct Connect

Explanation
Correct option:

S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations. As

data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path. S3 Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets. If you are uploading to a centralized bucket from geographically dispersed locations, or if you regularly transfer GBs or TBs of data across continents, you may save hours or days of data transfer time with S3 Transfer Acceleration.

Benefits of S3 Transfer Acceleration (S3TA):

via - https://aws.amazon.com/s3/transfer-acceleration/

Incorrect options:

Amazon CloudFront - Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is used for content delivery than for data uploads. CloudFront caches data and a subsequent request for a webpage will not go to the origin server, but will be served from the cache. S3 Transfer Acceleration is a better option for the given use-case.

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. You cannot use Direct Connect to optimize media uploads into S3.

AWS Global Accelerator - AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances. Similar to CloudFront it uses AWS Global network and edge locations for enhanced performance. It's an overall performance enhancer than an upload speed accelerator. You cannot use Global Accelerator to optimize media uploads into S3.

Reference:

https://aws.amazon.com/s3/transfer-acceleration/

Question 16: Correct
Which AWS service can be used to set up billing alarms to monitor estimated charges on your AWS account?

- AWS Cost Explorer

- AWS Organizations
- Amazon CloudWatch **(Correct)**
- Consolidated Billing

Explanation
Correct option:

Amazon CloudWatch

Amazon CloudWatch can be used to create an 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. These alerts are triggered by CloudWatch and messages are sent using Amazon Simple Notification Service (Amazon SNS). Billing metric data is stored in the US East (N. Virginia) Region and reflects worldwide charges.

The alarm triggers when your account billing exceeds the threshold you specify. It triggers only when actual billing exceeds the threshold. It doesn't use projections based on your usage so far in the month.

CloudWatch Billing Alarms
Overview:

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

Exam Alert:

It is useful to note the difference between CloudWatch Billing vs Budgets:

CloudWatch Billing Alarms: Sends an alarm when the actual cost exceeds a certain threshold.

Budgets: Sends an alarm when the actual cost exceeds the budgeted amount or even when the cost forecast exceeds the budgeted amount.

Incorrect options:

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. Billing alarms cannot be triggered via CloudTrail.

AWS Organizations - AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. Consolidated billing is a feature of AWS Organizations. You can use the master account of your organization to consolidate and pay for all member accounts. Billing alarms cannot, however, be triggered using Consolidated Billing.

AWS Cost Explorer - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. Cost Explorer will help analyze your data at a high level or dive deeper into your cost and usage data using various reports (Monthly costs by AWS service, hourly and resource Level cost). Billing alarms cannot be triggered via Cost Explorer.

Reference:

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

Question 17: Correct
Threat detection is of paramount importance for security in the Cloud. Which AWS service offers this key feature?

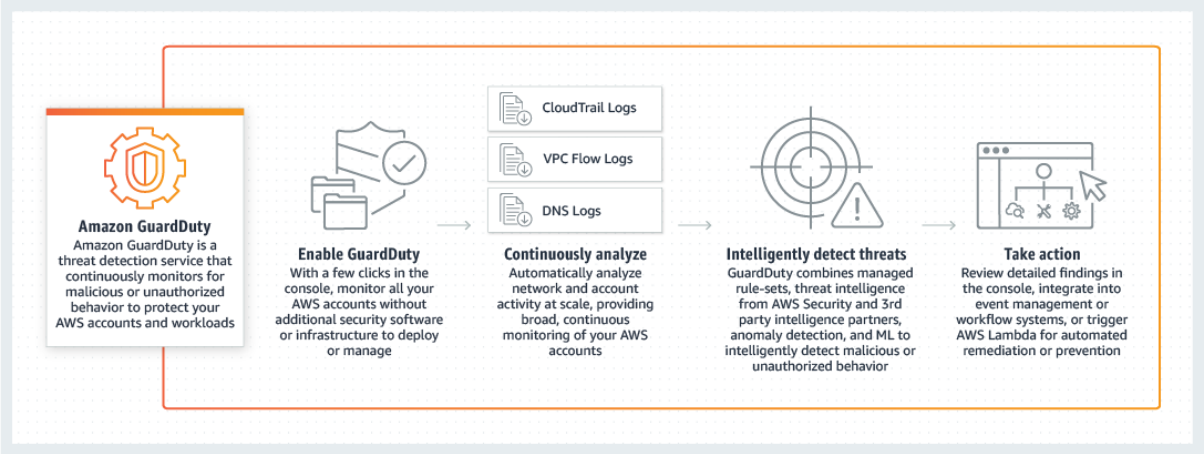
- AWS Shield
- Amazon GuardDuty **(Correct)**
- AWS CloudHSM
- Amazon Inspector

Explanation
Correct option:

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).

How GuardDuty Works:



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

Incorrect options:

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

AWS CloudHSM - AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your encryption keys on the AWS Cloud. With CloudHSM, you can manage your encryption keys using FIPS 140-2 Level 3 validated HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups.

Reference:

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

Question 18: Correct
AWS Marketplace facilitates which of the following use-cases? (Select two)

- [ ] Raise request for purchasing AWS Direct Connect connection

- ☐ Buy Amazon EC2 Standard Reserved Instances
- ☑ AWS customer can buy software that has been bundled into customized AMIs by the AWS Marketplace sellers **(Correct)**
- ☑ Sell Software as a Service (SaaS) solutions to AWS customers **(Correct)**
- ☐ Purchase compliance documents from third-party vendors

Explanation
Correct option:

Sell Software as a Service (SaaS) solutions to AWS customers

AWS customer can buy software that has been bundled into customized AMIs by the AWS Marketplace sellers

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. The AWS Marketplace enables qualified partners to market and sell their software to AWS Customers.

AWS Marketplace offers two ways for sellers to deliver software to customers: Amazon Machine Image (AMI) and Software as a Service (SaaS).

Amazon Machine Image (AMI): Offering an AMI is the preferred option for listing products in AWS Marketplace. Partners have the option for free or paid products. Partners can offer paid products charged by the hour or month. Bring Your Own License (BYOL) is also available and enables customers with existing software licenses to easily migrate to AWS.

Software as a Service (SaaS): If you offer a SaaS solution running on AWS (and are unable to build your product into an AMI) the SaaS listing offers our partners a way to market their software to customers.

Incorrect options:

Purchase compliance documents from third-party vendors - There is no third party vendor for providing compliance documents. AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements.

Buy Amazon EC2 Standard Reserved Instances - Amazon EC2 Standard Reserved Instances can be bought from the Amazon EC2 console at https://console.aws.amazon.com/ec2/

Raise request for purchasing AWS Direct Connect connection - AWS Direct Connect connection can be raised from the AWS management console at https://console.aws.amazon.com/directconnect/v2/home

References:

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

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

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-concepts-buying.html#ri-queued-purchase

Question 19: Correct
Which of the following is the best practice for application architecture on AWS Cloud?

- Build tightly coupled components
- Build monolithic applications
- Build loosely coupled components **(Correct)**
- Use synchronous communication between components

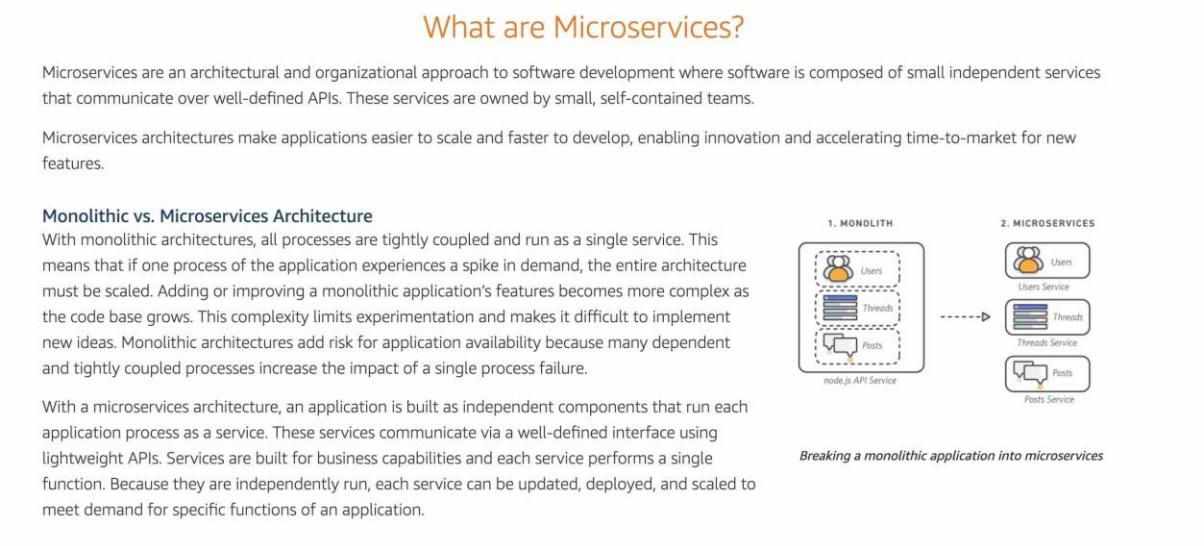
Explanation
Correct option:

Build loosely coupled components

AWS Cloud recommends microservices as an architectural and organizational approach to software development where software is composed of small independent services that communicate over well-defined APIs. These services are owned by small, self-contained teams.

Microservices architectures make applications easier to scale and faster to develop, enabling innovation and accelerating time-to-market for new features. Each service can be considered as a loosely coupled component of a bigger system. You can use services like SNS or SQS to decouple and scale microservices.

Microservices
Overview:



via - https://aws.amazon.com/blogs/compute/understanding-asynchronous-messaging-for-microservices/

Incorrect options:

Build tightly coupled components

Build monolithic applications

With monolithic architectures, all processes are tightly coupled and run as a single service. This means that if one process of the application experiences a spike in demand, the entire architecture must be scaled. Monolithic architectures add risk for application availability because many dependent and tightly coupled processes increase the impact of a single process failure. So both these options are incorrect.

Use synchronous communication between components - Synchronous between applications can be problematic if there are sudden spikes of traffic. You should use SNS or SQS to decouple your application components.

Reference:

https://aws.amazon.com/blogs/compute/understanding-asynchronous-messaging-for-microservices/

Question 20: Correct
Which of the following S3 storage classes do not charge any data retrieval fee? (Select two)

- [x] S3 Intelligent-Tiering
(Correct)
- [ ] S3 Standard-IA
- [ ] S3 Glacier

- ☐ S3 One Zone-IA
- ☑ S3 Standard **(Correct)**

Explanation
Correct options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. S3 Standard offers low latency and high throughput performance, It is designed for durability of 99.999999999% of objects across multiple Availability Zones. S3 Standard does not charge any data retrieval fee.

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 Intelligent-Tiering does not charge any data retrieval fee.

Please review this illustration for the S3 Storage Classes retrieval fee. You don't need to memorize the actual numbers, just remember that S3 Standard and S3 Intelligent-Tiering do not charge any retrieval
fee:

	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 Glacier - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. S3 Glacier has a data retrieval fee.

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. S3 One Zone-IA has a data retrieval fee.

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

Reference:

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

Question 21: Correct
Which pillar of AWS Well-Architected Framework is responsible for making sure that you focus on continually improving your processes and procedures?

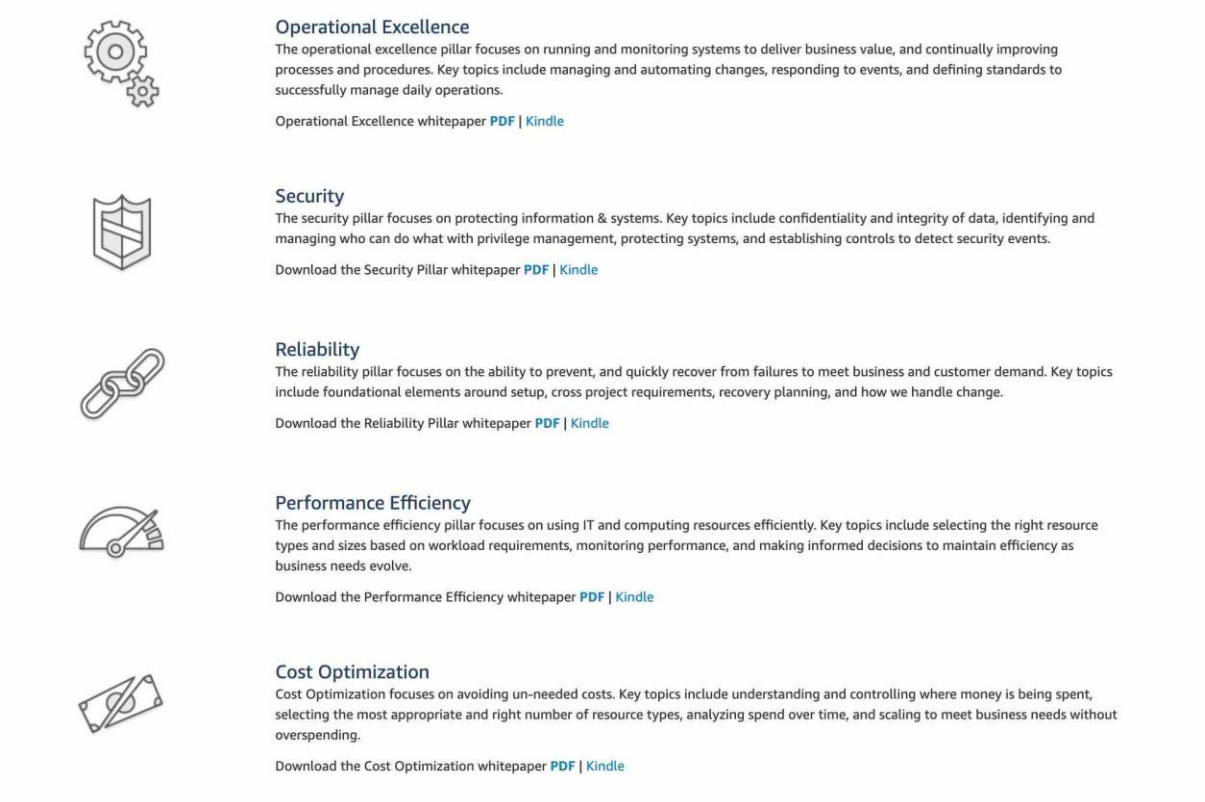
- Cost Optimization
- Performance Efficiency
- Reliability
- Operational Excellence **(Correct)**

Explanation
Correct option:

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.

Overview of the five pillars of the Well-Architected Framework:



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

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.

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.

Reliability - This refers to the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

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

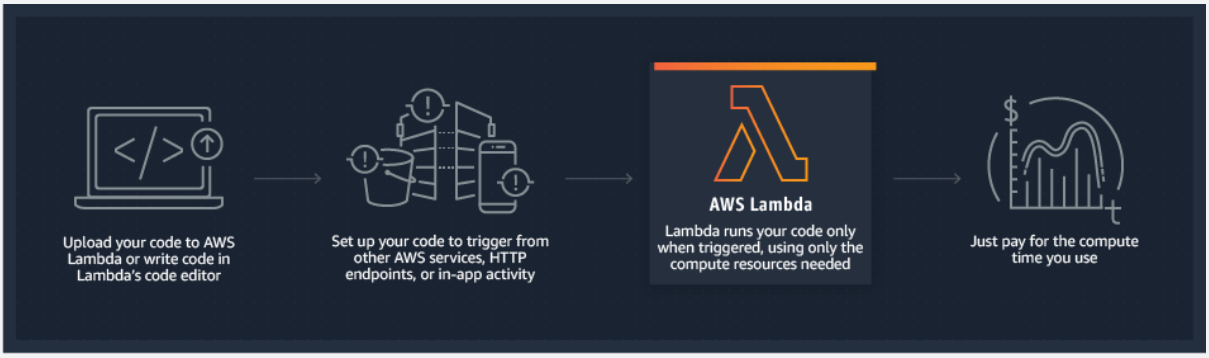
Question 22: Correct
A social media analytics company wants to migrate to a serverless stack on AWS. Which of the following scenarios can be handled by AWS Lambda? (Select two)

- [x] Lambda can be used for preprocessing of data before it is stored in Amazon S3 buckets **(Correct)**
- [ ] You can install low latency databases on Lambda
- [x] Lambda can be used to execute code in response to events such as updates to DynamoDB tables **(Correct)**
- [ ] Lambda can be used to store sensitive environment variables
- [ ] You can install Container Services on Lambda

Explanation
Correct options:

AWS Lambda lets you run code without provisioning or managing servers (Lambda is serverless). 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. This functionality makes it an extremely useful service capable of being a serverless backend for websites, data preprocessing, real-time data transformations when used with streaming data, etc.

How Lambda Works:



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

Lambda can be used to execute code in response to events such as updates to DynamoDB tables - Lambda can be configured to execute code in response to events, such as changes to Amazon S3 buckets, updates to an Amazon DynamoDB table, or custom events generated by your applications or devices.

Lambda can be used for preprocessing of data before it is stored in Amazon S3 buckets - Lambda can be used to run preprocessing scripts to filter, sort or transform data before sending it to downstream applications/services.

Incorrect options:

You can install low latency databases on Lambda - Lambda is serverless, so the underlying hardware and its working is not exposed to the customer. Installing software is not possible since we do not have access to the actual physical server on which Lambda executes the code.

You can install Container Services on Lambda - As discussed above, Lambda cannot be used for installing any software, since the underlying hardware/software might change for each request. But, it is possible to set an environment with necessary libraries when running scripts on Lambda.

Lambda can be used to store sensitive environment variables - Lambda is not a storage service and does not offer capabilities to store data. However, it is possible to read and decrypt/encrypt data using scripts in Lambda.

Reference:

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

Question 23: Correct
Which AWS service will help you install code automatically to an Amazon EC2 instance?

- AWS CodeBuild
- AWS Elastic Beanstalk
- AWS CodeDeploy **(Correct)**
- AWS CloudFormation

Explanation
Correct option:

AWS CodeDeploy

AWS CodeDeploy is a service that automates application deployments to a variety of compute services including Amazon EC2, AWS Fargate, AWS Lambda, and on-premises instances. CodeDeploy fully automates your application deployments eliminating the need for manual operations. CodeDeploy protects your application from downtime during deployments through rolling updates and deployment health tracking.

Incorrect options:

AWS Elastic Beanstalk - AWS Elastic Beanstalk is the fastest and simplest way to get web applications up and running on AWS. Developers simply upload their application code and the service automatically handles all the details such as resource provisioning, load balancing, auto-scaling, and monitoring. Elastic Beanstalk is an end-to-end application platform, unlike CodeDeploy, which is targeted at code deployment automation for any environment (Development, Testing, Production). It cannot be used to automatically deploy code to an Amazon EC2 instance.

AWS CloudFormation - AWS CloudFormation provides a common language for you to model and provision AWS and third-party application resources in your cloud environment. AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. It cannot be used to automatically deploy code to an Amazon EC2 instance.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue. It cannot be used to automatically deploy code to an Amazon EC2 instance.

Reference:

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

Question 24: Correct
A multi-national organization has separate VPCs for each of its business units on the AWS Cloud. The organization also wants to connect its on-premises data center with all VPCs for better organization-wide collaboration. Which AWS services can be combined to build the MOST efficient solution for this use-case? (Select two)

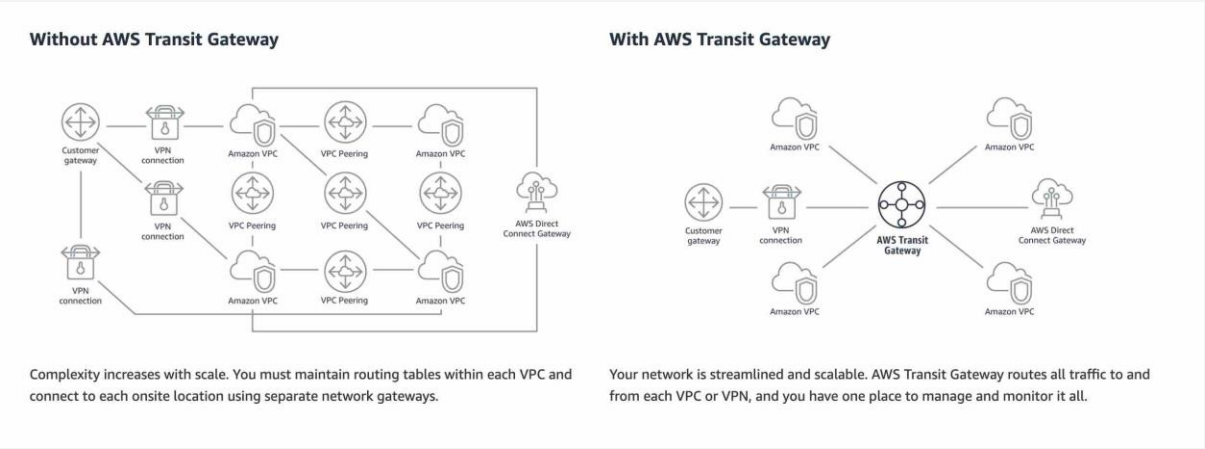
- [x] AWS Direct Connect **(Correct)**
- [ ] VPC Peering
- [ ] AWS Internet Gateway
- [ ] AWS Storage Gateway
- [x] AWS Transit Gateway **(Correct)**

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:



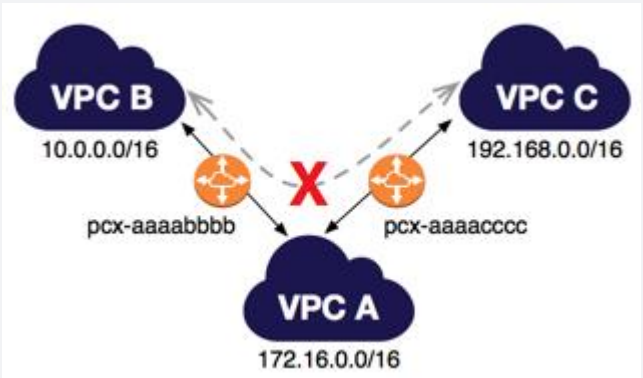
via - https://aws.amazon.com/transit-gateway/

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. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

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

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. You cannot use Internet Gateway to connect your on-premises data center with multiple VPCs within your AWS network.

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). You cannot use Storage Gateway to connect your on-premises data center with multiple VPCs within your AWS network.

Reference:

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

Question 25: Correct
Which benefit of Cloud Computing allows AWS to offer lower pay-as-you-go prices as usage from hundreds of thousands of customers is aggregated in the cloud?

- Massive economies of scale **(Correct)**
- Go global in minutes
- Trade capital expense for variable expense
- Increased speed and agility

Explanation
Correct option:

Massive economies of scale

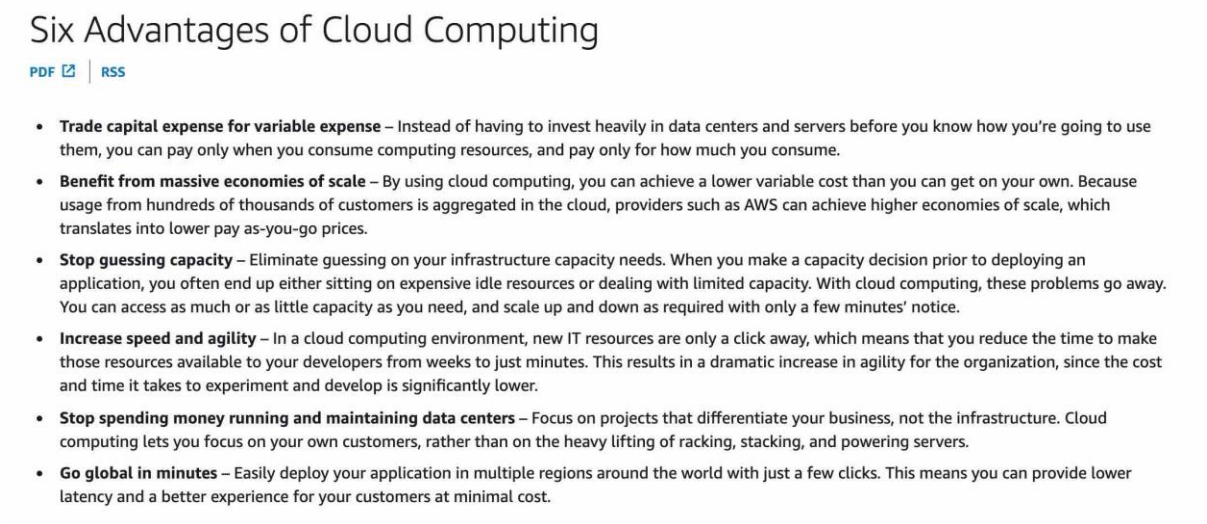
Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis.

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

Exam Alert:

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

premises
setup:



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

Incorrect options:

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

Increased Speed and Agility - In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization since the cost and time it takes to experiment and develop is significantly lower.

Go Global in minutes - Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide lower latency and a better experience for your customers at minimal cost.

Although these three options are also benefits of Cloud Computing, it is the massive economies of scale that allow AWS to offer lower pay-as-you-go prices as usage from hundreds of thousands of customers is aggregated in the cloud.

References:

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

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

Question 26: Correct
Which AWS service can be used to create a Content Distribution Network (CDN) on AWS Cloud?

- Amazon Route 53
- Amazon CloudFront **(Correct)**
- S3 Transfer Acceleration
- AWS Global Accelerator

Explanation
Correct option:

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. CloudFront is used for content delivery than for data uploads. CloudFront caches data and a subsequent request for a webpage will not go to the origin server, but will be served from the cache. S3 Transfer Acceleration is a better option for the given use-case.

Incorrect options:

Amazon Route 53 - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. You cannot use Route 53 to create a Content Distribution Network (CDN) on AWS Cloud.

AWS Global Accelerator - AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances. Similar to CloudFront it uses AWS Global network and edge locations for enhanced performance. It's an overall performance enhancer than an upload speed accelerator. You cannot use Global Accelerator to create a Content Distribution Network (CDN) on AWS Cloud.

S3 Transfer Acceleration - Amazon S3 Transfer Acceleration (S3TA) enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path. S3 Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets. You cannot use Transfer Acceleration to create a Content Distribution Network (CDN) on AWS Cloud.

Reference:

https://aws.amazon.com/cloudfront/

Question 27: Correct
As per the AWS Shared Responsibility Model, which of the following is a responsibility of AWS from a security and compliance point of view?

- Patching guest OS and applications
- Service and Communications Protection
- Identity and Access Management
- Patching networking infrastructure **(Correct)**

Explanation
Correct option:

Patching networking infrastructure

According to the AWS Shared Responsibility Model, AWS is responsible for "Security of the Cloud". This includes protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Therefore, patching networking infrastructure is the responsibility of AWS.

Incorrect options:

Service and Communications Protection

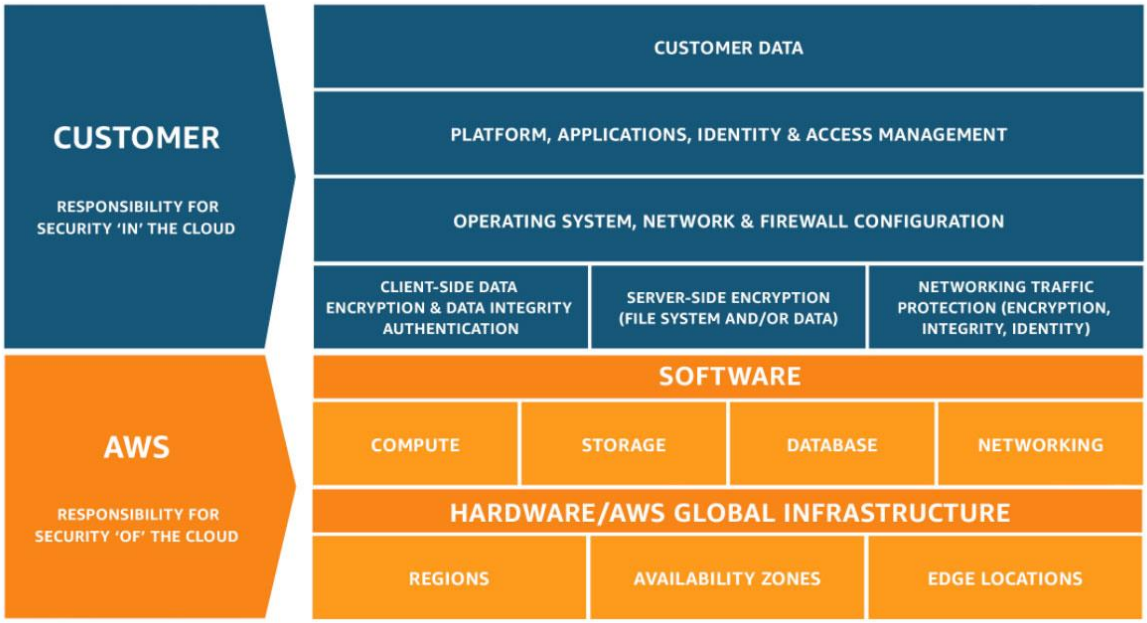
Identity and Access Management

Patching guest OS and applications

The customer is responsible for security "in" the cloud. This covers things such as services and communications protection; Identity and Access Management; and patching guest OS and applications. Customers are responsible for managing their data including encryption options and using Identity and Access Management tools for implementing appropriate access control policies as per their organization requirements. Therefore, these three options fall under the responsibility of the customer according to the AWS shared responsibility model.

Exam Alert:

Please review the Shared Responsibility Model in detail as you can expect multiple questions on the shared responsibility model in the
exam:



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

Reference:

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

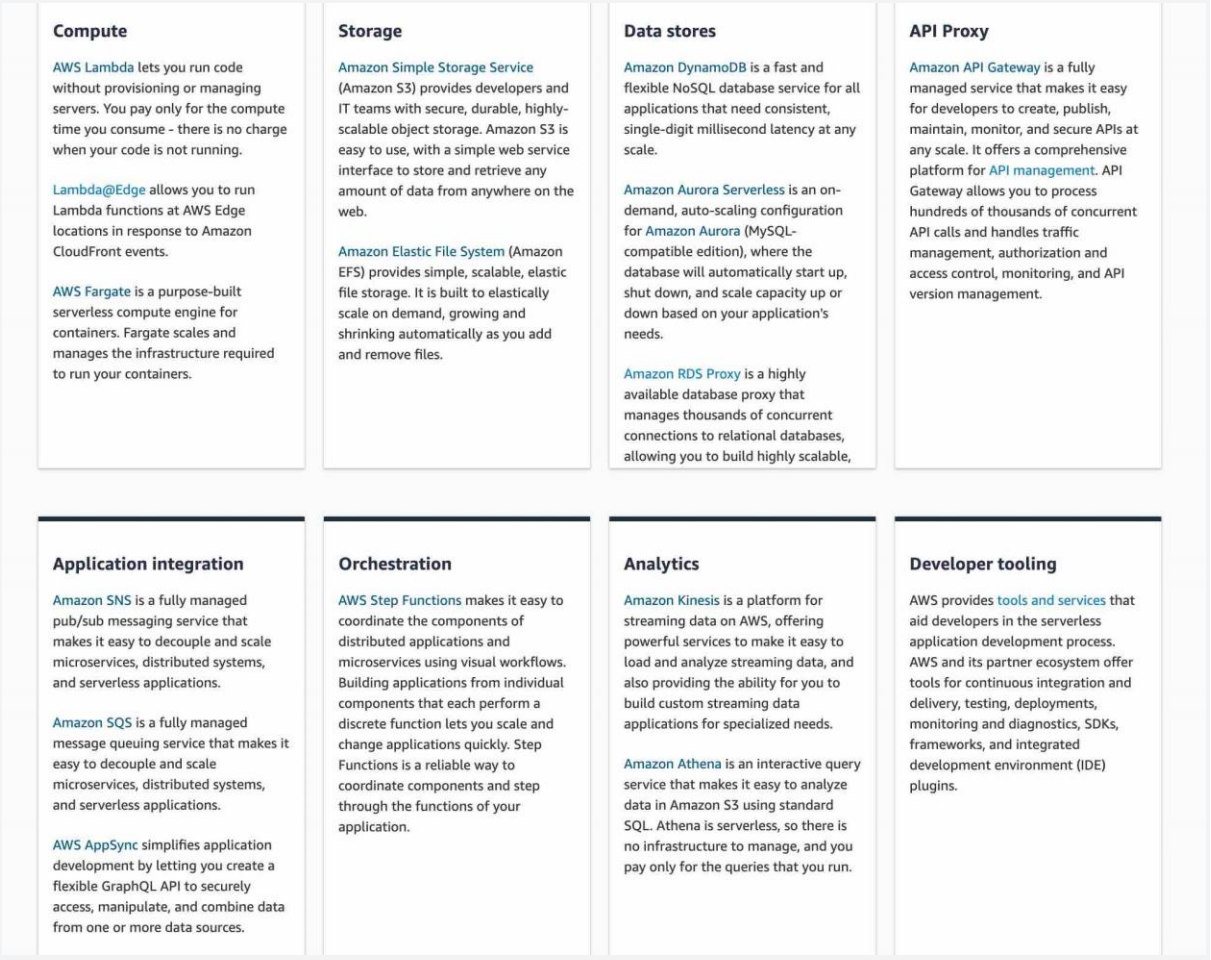
Question 28: Correct
Which of the following are the serverless computing services offered by AWS (Select two)

- [x] AWS Lambda
  (Correct)
- [x] AWS Fargate
  (Correct)
- [ ] Amazon Lightsail
- [ ] AWS Elastic Beanstalk
- [ ] Amazon Elastic Compute Cloud (EC2)

Explanation
Correct options:

Serverless is the native architecture of the cloud that enables you to shift more of your operational responsibilities to AWS, increasing your agility and innovation. Serverless allows you to build and run applications and services without thinking about servers. It eliminates infrastructure management tasks such as server or cluster provisioning, patching, operating system maintenance, and capacity provisioning.

The AWS serverless platform overview:



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

AWS Lambda - 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 set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running.

AWS Fargate - AWS Fargate is a serverless compute engine for containers that 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.

AWS Fargate is a purpose-built serverless compute engine for containers. Fargate scales and manages the infrastructure required to run your containers.

Incorrect options:

Amazon Elastic Compute Cloud (EC2) - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.

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

Amazon Lightsail - Lightsail is an easy-to-use cloud platform that offers you everything needed to build an application or website, plus a cost-effective, monthly plan. Lightsail offers several preconfigured, one-click-to-launch operating systems, development stacks, and web applications, including Linux, Windows OS, and WordPress.

References:

https://aws.amazon.com/serverless/

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

Question 29: **Correct**
Which of the following is a container service of AWS?

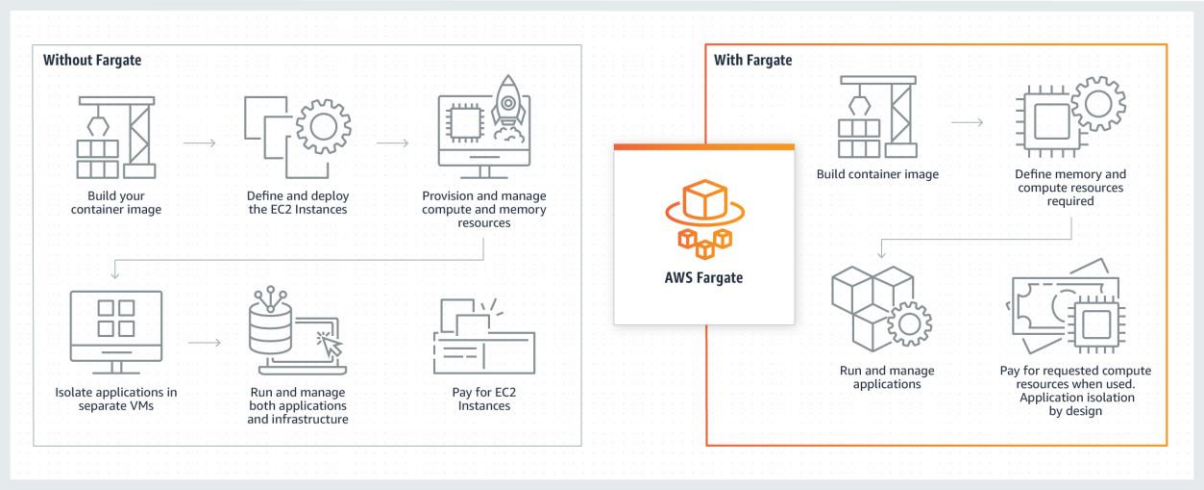
- Amazon SageMaker
- AWS Elastic Beanstalk
- Amazon Simple Notification Service
- AWS Fargate **(Correct)**

Explanation
Correct option:

AWS Fargate

AWS Fargate is a serverless compute engine for containers that 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.

How Fargate Works:



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

Incorrect options:

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

Amazon Simple Notification Service - Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

Amazon SageMaker - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models.

Reference:

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

Question 30: Correct

The DevOps team at a Big Data consultancy has set up EC2 instances across two AWS Regions for its flagship application. Which of the following characterizes this application architecture?

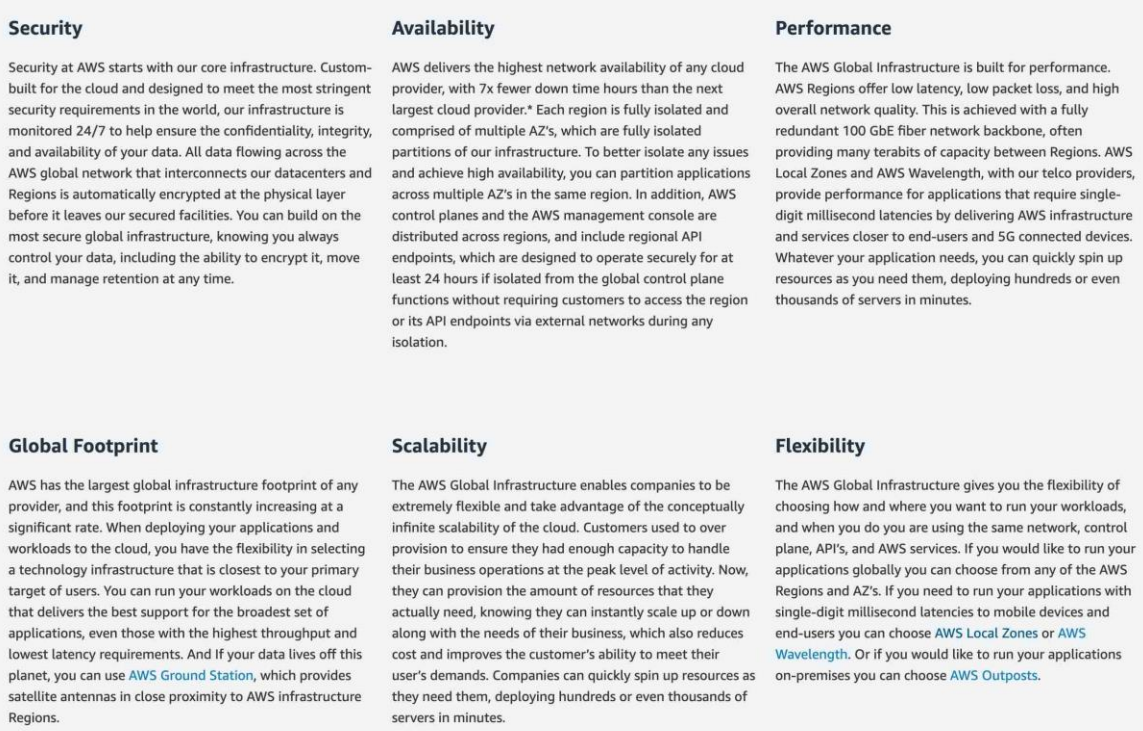
- Deploying the application across two AWS Regions improves scalability
- Deploying the application across two AWS Regions improves security
- Deploying the application across two AWS Regions improves agility

- Deploying the application across two AWS Regions improves availability **(Correct)**

Explanation
Correct option:

Deploying the application across two AWS Regions improves availability - Highly available systems are those that can withstand some measure of degradation while remaining available. Each AWS Region is fully isolated and comprised of multiple Availability Zones (AZ's), which are fully isolated partitions of AWS infrastructure. To better isolate any issues and achieve high availability, you can partition applications across multiple AZ's in the same AWS Region or even across multiple AWS Regions.

Key Benefits of AWS Global Infrastructure:



Security

Security at AWS starts with our core infrastructure. Custom-built for the cloud and designed to meet the most stringent security requirements in the world, our infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of your data. All data flowing across the AWS global network that interconnects our datacenters and Regions is automatically encrypted at the physical layer before it leaves our secured facilities. You can build on the most secure global infrastructure, knowing you always control your data, including the ability to encrypt it, move it, and manage retention at any time.

Availability

AWS delivers the highest network availability of any cloud provider, with 7x fewer down time hours than the next largest cloud provider.* Each region is fully isolated and comprised of multiple AZ's, which are fully isolated partitions of our infrastructure. To better isolate any issues and achieve high availability, you can partition applications across multiple AZ's in the same region. In addition, AWS control planes and the AWS management console are distributed across regions, and include regional API endpoints, which are designed to operate securely for at least 24 hours if isolated from the global control plane functions without requiring customers to access the region or its API endpoints via external networks during any isolation.

Performance

The AWS Global Infrastructure is built for performance. AWS Regions offer low latency, low packet loss, and high overall network quality. This is achieved with a fully redundant 100 GbE fiber network backbone, often providing many terabits of capacity between Regions. AWS Local Zones and AWS Wavelength, with our telco providers, provide performance for applications that require single-digit millisecond latencies by delivering AWS infrastructure and services closer to end-users and 5G connected devices. Whatever your application needs, you can quickly spin up resources as you need them, deploying hundreds or even thousands of servers in minutes.

Global Footprint

AWS has the largest global infrastructure footprint of any provider, and this footprint is constantly increasing at a significant rate. When deploying your applications and workloads to the cloud, you have the flexibility in selecting a technology infrastructure that is closest to your primary target of users. You can run your workloads on the cloud that delivers the best support for the broadest set of applications, even those with the highest throughput and lowest latency requirements. And If your data lives off this planet, you can use AWS Ground Station, which provides satellite antennas in close proximity to AWS infrastructure Regions.

Scalability

The AWS Global Infrastructure enables companies to be extremely flexible and take advantage of the conceptually infinite scalability of the cloud. Customers used to over provision to ensure they had enough capacity to handle their business operations at the peak level of activity. Now, they can provision the amount of resources that they actually need, knowing they can instantly scale up or down along with the needs of their business, which also reduces cost and improves the customer's ability to meet their user's demands. Companies can quickly spin up resources as they need them, deploying hundreds or even thousands of servers in minutes.

Flexibility

The AWS Global Infrastructure gives you the flexibility of choosing how and where you want to run your workloads, and when you do you are using the same network, control plane, API's, and AWS services. If you would like to run your applications globally you can choose from any of the AWS Regions and AZ's. If you need to run your applications with single-digit millisecond latencies to mobile devices and end-users you can choose AWS Local Zones or AWS Wavelength. Or if you would like to run your applications on-premises you can choose AWS Outposts.

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

Incorrect options:

Deploying the application across two AWS Regions improves 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. Deploying the application across two AWS Regions does not improve agility.

Deploying the application across two AWS Regions improves security - The application security is dependent on multiple factors such as data encryption, IAM policies, IAM roles, VPC security configurations, Security Groups, NACLs, etc. Deploying the application across

two AWS Regions directly impacts availability. So this option is not the best fit for the given use-case.

Deploying the application across two AWS Regions improves scalability - For the given use-case, you can improve the scalability of the application by using an Application Load Balancer with an Auto Scaling group. Deploying the application across two AWS Regions directly impacts availability. So this option is not the best fit for the given use-case.

Reference:

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

Question 31: Correct
Which pillar of AWS Well-Architected Framework is responsible for making sure that you select the right resource types and sizes based on your workload requirements?

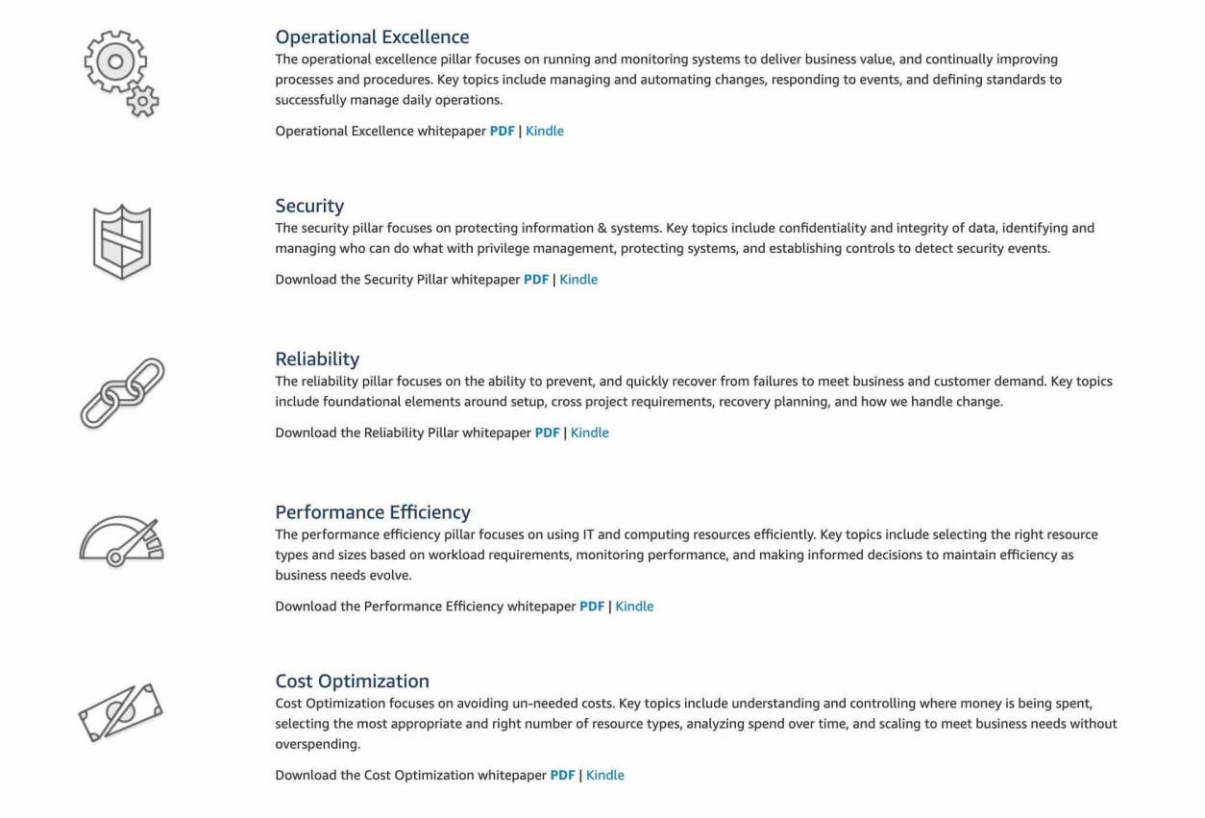
- Performance Efficiency **(Correct)**
- Reliability
- Cost Optimization
- Operational Excellence

Explanation
Correct option:

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.

Overview of the five pillars of the Well-Architected
Framework:



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

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.

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.

Reliability - This refers to the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

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.

Reference:

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

Question 32: Correct
Which of the following entities are part of a VPC in the AWS Cloud? (Select two)

- [x] Subnet
  (Correct)
- [ ] API Gateway
- [x] Internet Gateway
  (Correct)
- [ ] Storage Gateway
- [ ] Object

Explanation
Correct option:

Subnet

Internet Gateway

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

The following are the key concepts for VPCs:

Virtual private cloud (VPC) — A virtual network dedicated to your AWS account.

Subnet — A range of IP addresses in your VPC.

Route table — A set of rules, called routes, that are used to determine where network traffic is directed.

Internet Gateway — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.

VPC endpoint — Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Incorrect options:

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. Storage Gateway is not part of VPC.

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. API Gateway is not part of a VPC.

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

Reference:

https://docs.amazonaws.cn/en_us/vpc/latest/userguide/what-is-amazon-vpc.html

Question 33: **Correct**
A firm wants to maintain the same data on S3 between its production account and multiple test accounts. Which technique should you choose to copy data into multiple test accounts while retaining object metadata?

- Amazon S3 Storage Classes
- Amazon S3 Transfer Acceleration
- Amazon S3 Bucket Policy
- Amazon S3 Replication **(Correct)**

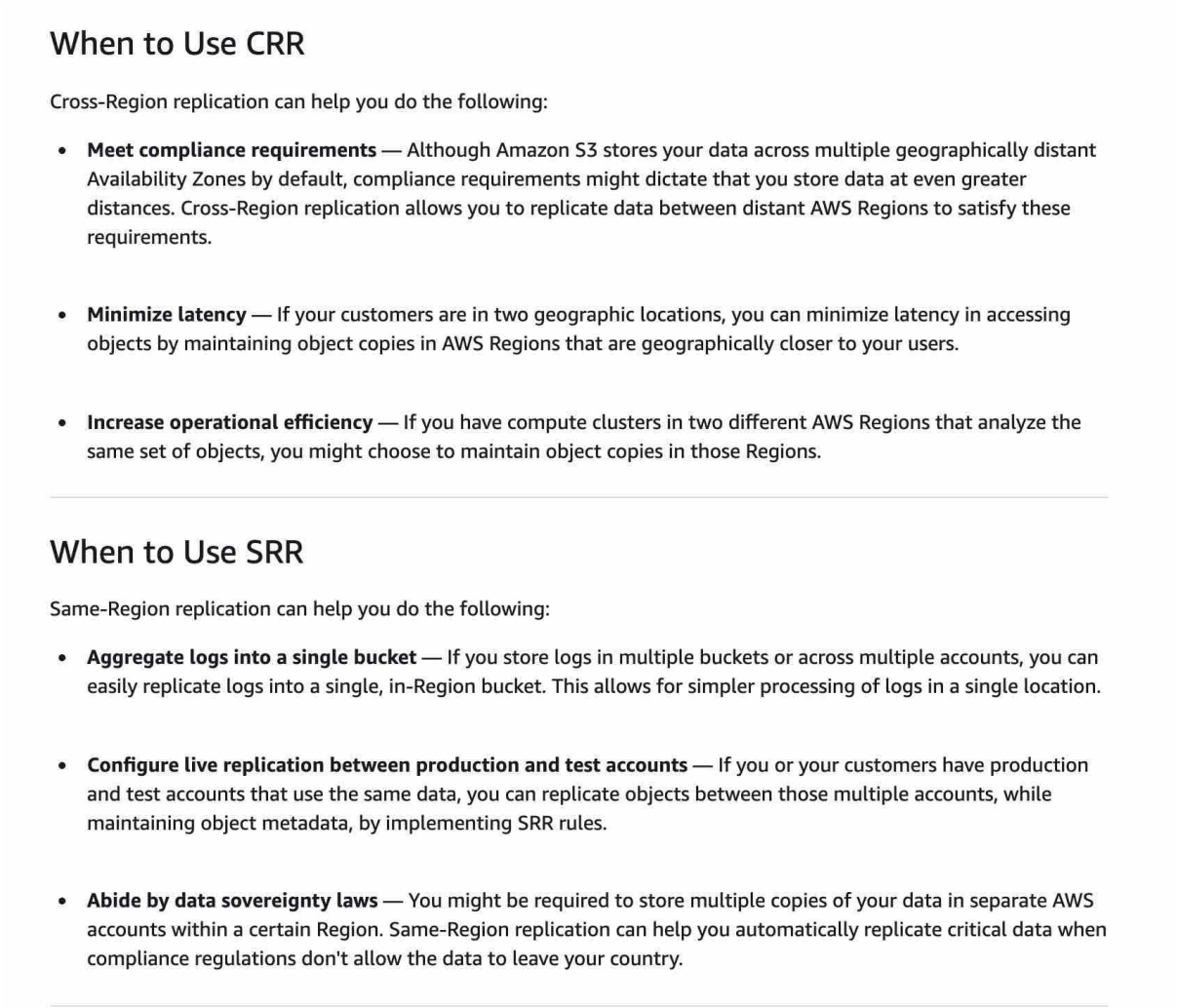
Explanation
Correct option:

Amazon S3 Replication

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. You can use replication to make copies of your objects that retain all metadata, such as the original object creation time and version IDs. This capability is important if you need to ensure that your replica is identical to the source object.

Exam Alert:

Amazon S3 supports two types of replication: Cross Region Replication vs Same Region Replication. 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

Incorrect options:

Amazon S3 Bucket Policy - A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates. You cannot replicate data using a bucket policy.

Amazon 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. This facility speeds up access between end-user and S3, this is not for replicating data.

Amazon S3 Storage Classes - Amazon S3 offers a range of storage classes designed for different use cases. Each storage class has a defined set of rules to store, encrypt data at a certain price. Based on the use case, customers can choose the storage class that best suits their business requirements.

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. You cannot replicate data using storage classes.

Reference:

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

Question 34: Correct
AWS Organizations provides which of the following benefits? (Select two)

- ☐ Provision EC2 Spot instances across the member AWS accounts
- ☑ Share the reserved EC2 instances amongst the member AWS accounts **(Correct)**
- ☐ Deploy patches on EC2 instances across the member AWS accounts
- ☐ Check vulnerabilities on EC2 instances across the member AWS accounts
- ☑ Volume discounts for Amazon EC2 and Amazon S3 aggregated across the member AWS accounts **(Correct)**

Explanation
Correct option:

Volume discounts for Amazon EC2 and Amazon S3 aggregated across the member AWS accounts

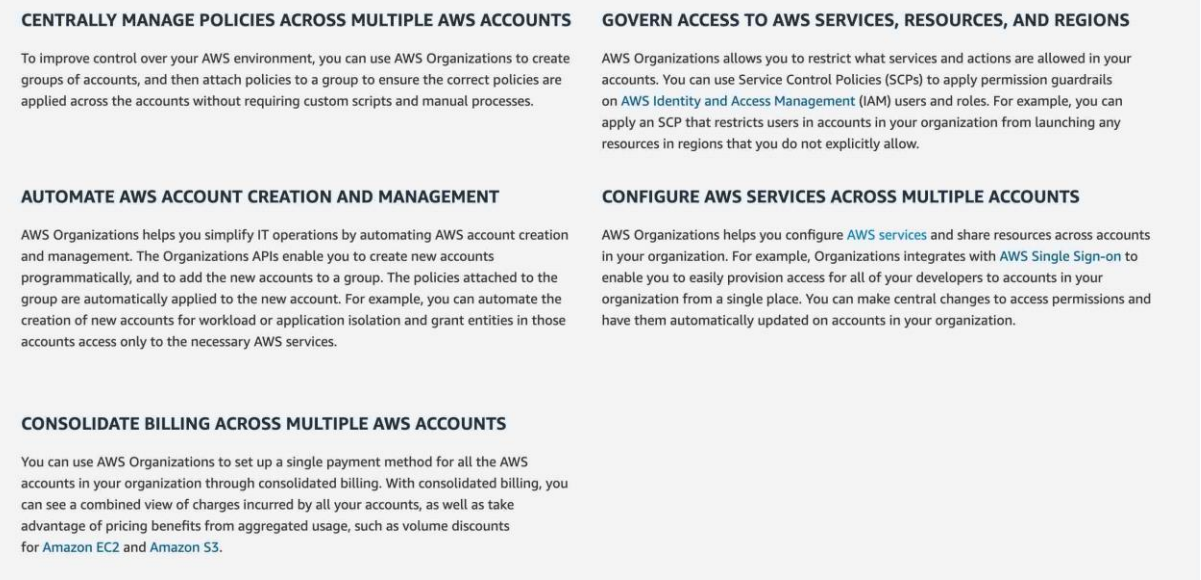
Share the reserved EC2 instances amongst the member AWS accounts

AWS Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources such as reserved EC2 instances 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.

You can use AWS Organizations to set up a single payment method for all the AWS accounts in your organization through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for Amazon EC2 and Amazon S3.

Key benefits of AWS Organizations:



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

Incorrect options:

Check vulnerabilities on EC2 instances across the member AWS accounts

Deploy patches on EC2 instances across the member AWS accounts

Provision EC2 Spot instances across the member AWS accounts

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

Reference:

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

Question 35: Correct

Which AWS service can be used to host a static website with the LEAST effort?

- Amazon Elastic File System (Amazon EFS)
- AWS Storage Gateway
- Amazon Simple Storage Service (Amazon S3) **(Correct)**
- Amazon S3 Glacier

Explanation

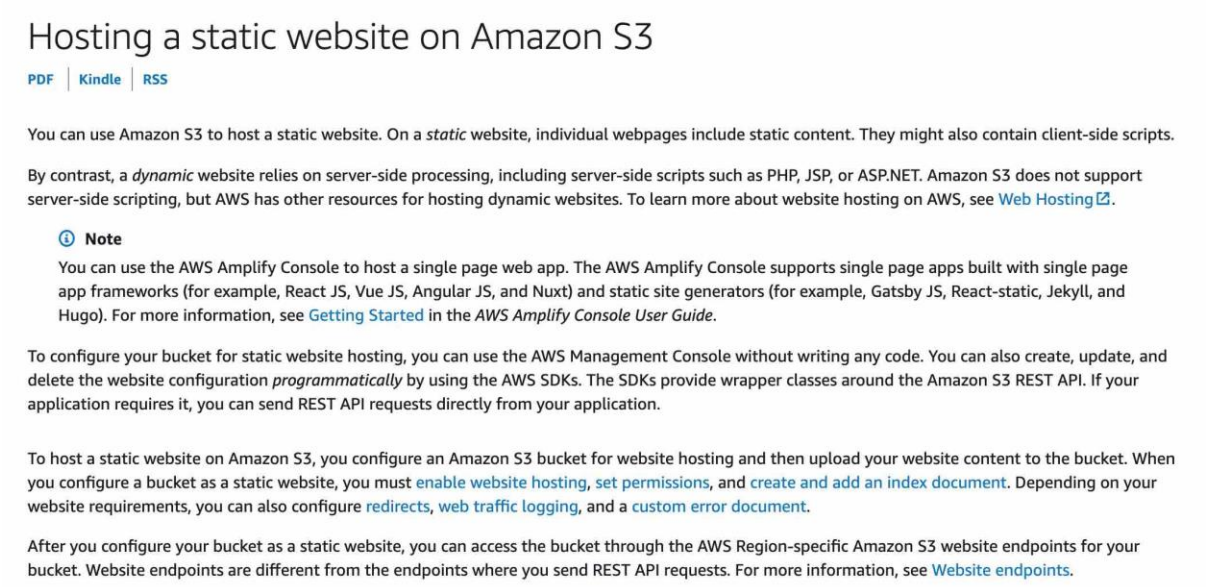
Correct option:

Amazon Simple Storage Service (Amazon S3)

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3's flat, non-hierarchical structure and various management features are helping customers of all sizes and industries organize their data in ways that are valuable to their businesses and teams.

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.

Note

You can use the AWS Amplify Console to host a single page web app. The AWS Amplify Console supports single page apps built with single page app frameworks (for example, React JS, Vue JS, Angular JS, and Nuxt) and static site generators (for example, Gatsby JS, React-static, Jekyll, and Hugo). For more information, see Getting Started in the *AWS Amplify Console User Guide*.

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

Incorrect options:

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. It helps on-premises applications to access data on AWS Cloud. It cannot be used to host a website.

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. EFS storage option cannot directly be used to host a website, EFS needs to be mounted on Amazon EC2 to work as a static website.

Amazon 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. As you see, this cannot be used for hosting a website.

Reference:

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

Question 36: Correct
AWS Trusted Advisor can provide alerts on which of the following common security misconfigurations? (Select two)?

- ☐ When you share IAM user credentials with others
- ☑ When you don't turn on user activity logging (AWS CloudTrail) **(Correct)**
- ☑ When you allow public access to Amazon S3 buckets **(Correct)**
- ☐ When you don't enable data encryption on S3 Glacier
- ☐ When you don't tag objects in S3 buckets

Explanation
Correct options:

When you allow public access to Amazon S3 buckets

When you don't turn on user activity logging (AWS CloudTrail)

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.

Trusted Advisor inspects your AWS environment and makes recommendations when opportunities may exist to save money, improve system performance, or close security gaps. It provides alerts on several of the most common security misconfigurations that can occur, including leaving certain ports open that make you vulnerable to hacking and unauthorized access, neglecting to create IAM accounts for your internal users, allowing public access to Amazon S3 buckets, not turning on user activity logging (AWS CloudTrail), or not using MFA on your root AWS Account.

How Trusted Advisor
Works:

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

Incorrect options:

When you don't tag objects in S3 buckets - Tagging objects (or any resource) in S3 is not mandatory and it's not a security threat.

"When you share IAM user credentials with others" - It is the customer's responsibility to adhere to the IAM security best practices and never share the IAM user credentials with others. Trusted Advisor cannot send an alert for such use-cases.

When you don't enable data encryption on S3 Glacier - By default, data on S3 Glacier is encrypted. So, this option has been added as a distractor.

Reference:

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

Question 37: Correct
Amazon EC2 Spot instances are a best-fit for which of the following scenarios?

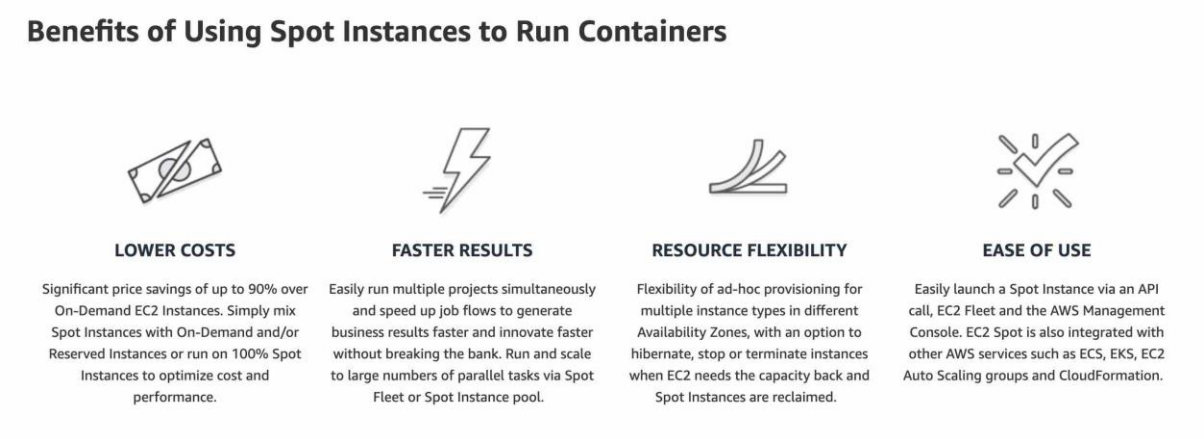
- To run scheduled jobs (jobs that run at the same time every day)
- To run batch processes for critical workloads
- To run any containerized workload with Elastic Container Service (ECS) that can be interrupted **(Correct)**
- To install cost-effective RDS database

Explanation
Correct option:

To run any containerized workload with Elastic Container Service (ECS) that can be interrupted

Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices.

Containers are stateless, fault-tolerant and a great fit for Spot Instances. Spot Instances can be used with Elastic Container Service (ECS) or Elastic Container Service for Kubernetes (EKS) to run any containerized workload, from distributed parallel test systems to applications that map millions of miles a day. Spot instances provide the flexibility of ad-hoc provisioning for multiple instance types in different Availability Zones, with an option to hibernate, stop or terminate instances when EC2 needs the capacity back and Spot Instances are reclaimed.



via - https://aws.amazon.com/ec2/spot/containers-for-less/

Incorrect options:

To install cost-effective RDS database - Spot instance capacity allocated to you can be taken back anytime without notice if AWS needs them. Hence, Spot instances can only be used as additional compute capacity and not for hosting or installing any software or database.

To run batch processes for critical workloads - Business-critical workloads cannot be run on Spot instances.

To run scheduled jobs (jobs that run at the same time every day) - There is no guarantee that a Spot instance will be available at a specific time every day. For a scheduled requirement, Scheduled Reserved instances should be used.

Reference:

https://aws.amazon.com/ec2/spot/containers-for-less/

Question 38: Correct
A social media company wants to have the MOST cost-optimal strategy for deploying EC2 instances. As a Cloud Practitioner, which of the following options would you recommend? (Select two)

- [ ]

Use On-Demand Instances for ad-hoc jobs that can be interrupted

- [x] Use Spot Instances for ad-hoc jobs that can be interrupted **(Correct)**
- [ ] Use Reserved Instances for ad-hoc jobs that can be interrupted
- [x] Use Reserved Instances to run applications with a predictable usage over the next one year **(Correct)**
- [ ] Use On-Demand Instances to run applications with a predictable usage over the next one year

Explanation
Correct options:

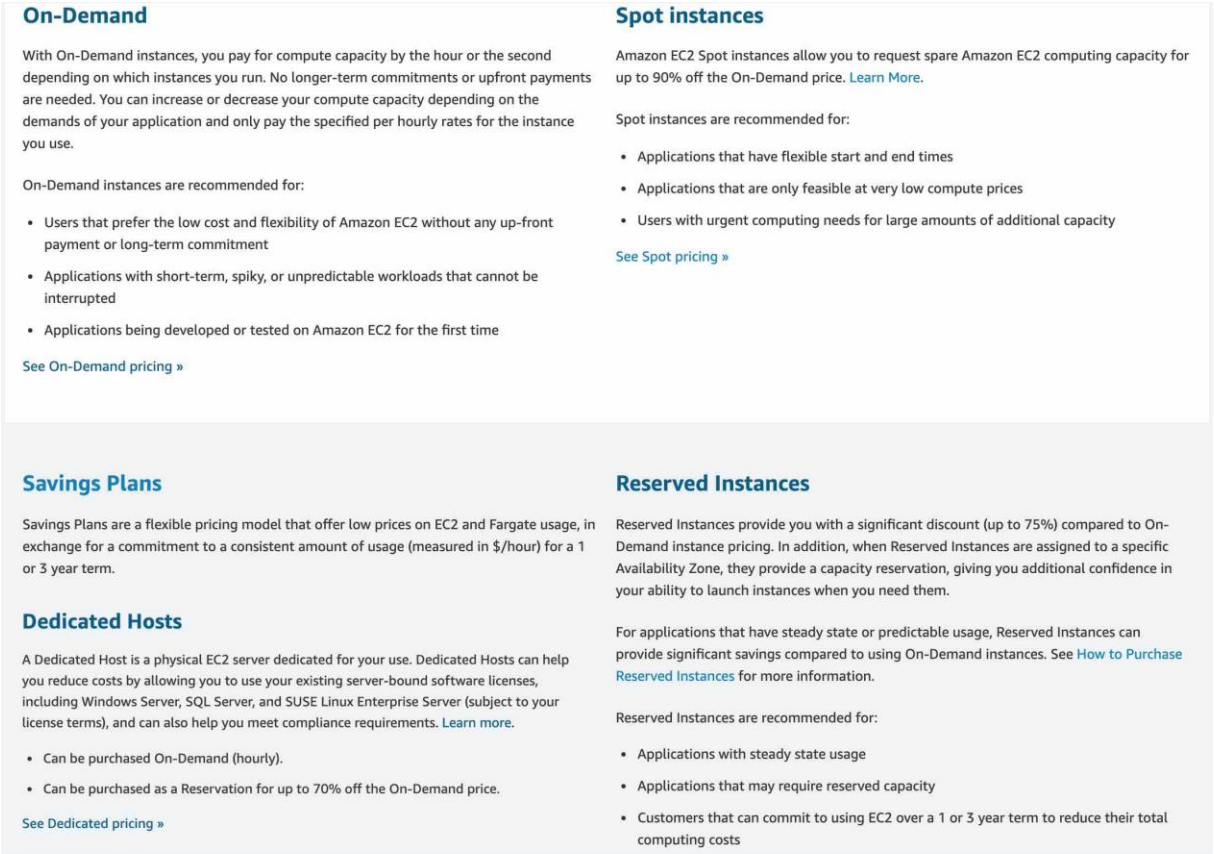
Use Spot Instances for ad-hoc jobs that can be interrupted

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 optional tasks. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time.

Use Reserved Instances to run applications with a predictable usage over the next one year

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 are a great fit for application with a steady-state usage. Reserved instances cannot be interrupted.

EC2 Pricing Options
Overview:



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

Incorrect options:

Use On-Demand Instances to run applications with a predictable usage over the next one year

Use On-Demand Instances for ad-hoc jobs that can be interrupted

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 or Reserved instances, so both these options are not correct.

Use Reserved Instances for ad-hoc jobs that can be interrupted - Spot instances are more cost-effective than Reserved instances for running ad-hoc jobs that can be interrupted, so this option is not correct.

Reference:

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

Question 39: **Correct**

Which of the following entities should be used for an Amazon EC2 Instance to access a DynamoDB table?

- Amazon Cognito
- AWS IAM user access keys
- IAM role **(Correct)**
- AWS Key Management Service

Explanation
Correct option:

IAM Role

An IAM Role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user in that it is an AWS identity with permissions policies that determine what the identity can and cannot do in AWS. When you assume a role, it provides you with temporary security credentials for your role session.

Incorrect options:

AWS IAM user access keys - Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Access keys consist of two parts: an access key ID and a secret access key. As a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. As a best practice, AWS suggests the use of temporary security credentials (IAM roles) instead of access keys.

Amazon Cognito - Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0. Amazon Cognito cannot be used to facilitate an Amazon EC2 Instance to access a DynamoDB table.

AWS Key Management Service - AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS cannot be used to facilitate an Amazon EC2 Instance to access a DynamoDB table.

Reference:

https://docs.amazonaws.cn/en_us/amazondynamodb/latest/developerguide/authentication-and-access-control.html

Question 40: Correct
AWS Shield Advanced provides expanded DDoS attack protection for web applications running on which of the following resources? (Select two)

- [ ] AWS Identity and Access Management (IAM)
- [x] Amazon Elastic Compute Cloud **(Correct)**
- [x] Amazon CloudFront **(Correct)**
- [ ] Amazon Simple Storage Service (Amazon S3)
- [ ] AWS Elastic Beanstalk

Explanation
Correct options:

Amazon CloudFront

Amazon Elastic Compute Cloud

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

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

Incorrect options:

Amazon Simple Storage Service (Amazon S3)

AWS Elastic Beanstalk

AWS Identity and Access Management (IAM)

These three resource types are not supported by AWS Shield Advanced.

Reference:

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

Question 41: Correct
Which of the following is available across all AWS Support plans?

- Full set of AWS Trusted Advisor best practice checks
- Enhanced Technical Support with unlimited cases and unlimited contacts
- Third-Party Software Support
- AWS Personal Health Dashboard **(Correct)**

Explanation
Correct option:

"AWS Personal Health Dashboard"

Full set of AWS Trusted Advisor best practice checks, enhanced Technical Support with unlimited cases, and unlimited contacts and third-party Software Support are available only for Business and Enterprise Support plans.

AWS Personal Health Dashboard is available for all Support plans.

Exam Alert:

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

	Developer	Business	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Recommended if you have production workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
AWS Trusted Advisor Best Practice Checks	7 Core checks	Full set of checks	Full set of checks
Enhanced Technical Support	Business hours** email access to Cloud Support Associates Unlimited cases / 1 primary contact	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)
Case Severity / Response Times*	General guidance: < 24 business hours** System impaired: < 12 business hours**	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting

	Developer	Business	Enterprise
Proactive Programs		Access to Infrastructure Event Management for additional fee.	Infrastructure Event Management Well-Architected Reviews Operations Reviews Technical Account Manager (TAM) coordinates access to programs and other AWS experts as needed.
Technical Account Management			Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization.
Training			Access to online self-paced labs
Account Assistance			Concierge Support Team
Pricing	Greater of $29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of $100 / month*** - or - 10% of monthly AWS usage for the first $0–$10K 7% of monthly AWS usage from $10K–$80K 5% of monthly AWS usage from $80K–$250K 3% of monthly AWS usage over $250K See pricing detail and example.	Greater of $15,000 - or - 10% of monthly AWS usage for the first $0–$150K 7% of monthly AWS usage from $150K–$500K 5% of monthly AWS usage from $500K–$1M 3% of monthly AWS usage over $1M See pricing detail and example.

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

Incorrect options:

"Full set of AWS Trusted Advisor best practice checks"

"Enhanced Technical Support with unlimited cases and unlimited contacts"

"Third-Party Software Support"

As mentioned in the explanation above, these options are available only for Business and Enterprise Support plans.

Reference:

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

Question 42: **Incorrect**
How is Amazon EC2 different from traditional hosting systems? (Select two)

- ☐ Amazon EC2 can scale with changing computing requirements **(Correct)**
- ☑ Amazon EC2 caters more towards groups of users with similar system requirements so that the server resources are shared across multiple users and the cost is reduced **(Incorrect)**
- ☑ With Amazon EC2, developers can launch and terminate the instances anytime they need to **(Correct)**
- ☐ With Amazon EC2, users risk overbuying resources
- ☐ Amazon EC2 provides a pre-configured instance for a fixed monthly cost

Explanation
Correct options:

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud with support for per-second billing. It is the easiest way to provision servers on AWS Cloud and access the underlying OS.

Amazon EC2 differs fundamentally with the traditional on-premises hosting systems in the flexibility, control and significant cost savings it offers developers, allowing them to treat Amazon EC2 instance as their own customized server backed by the robust infrastructure of AWS Cloud.

Amazon EC2 can scale with changing computing requirements - When computing requirements unexpectedly change, Amazon EC2 can be scaled to match the requirements. Developers can control how many EC2 instances are in use at any given point in time.

With Amazon EC2, developers can launch and terminate the instances anytime they need to - Using Amazon EC2, developers can choose not only to launch, terminate, start or shut down instances at any time, but they can also completely customize the configuration of their instances to suit their needs.

Incorrect options:

Amazon EC2 provides a pre-configured instance for a fixed monthly cost - This is an incorrect option. EC2 developers enjoy the benefit of paying only for their actual resource consumption with no monthly or upfront costs. Developers can customize their EC2 instances for their application stack.

With Amazon EC2, users risk overbuying resources - This is an incorrect statement. Users risk overbuying in traditional hosting services where users pay a fixed, up-front fee irrespective of their actual computing power used. With EC2, users pay only for the actual resources consumed.

Amazon EC2 caters more towards groups of users with similar system requirements so that the server resources are shared amongst multiple users and the cost is reduced - This is an incorrect statement. Resources are not shared between users in EC2, which is why the users have the flexibility to start or shutdown the instances as per their requirement. This is not possible for the traditional hosting systems where the resources are shared across users.

Reference:

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

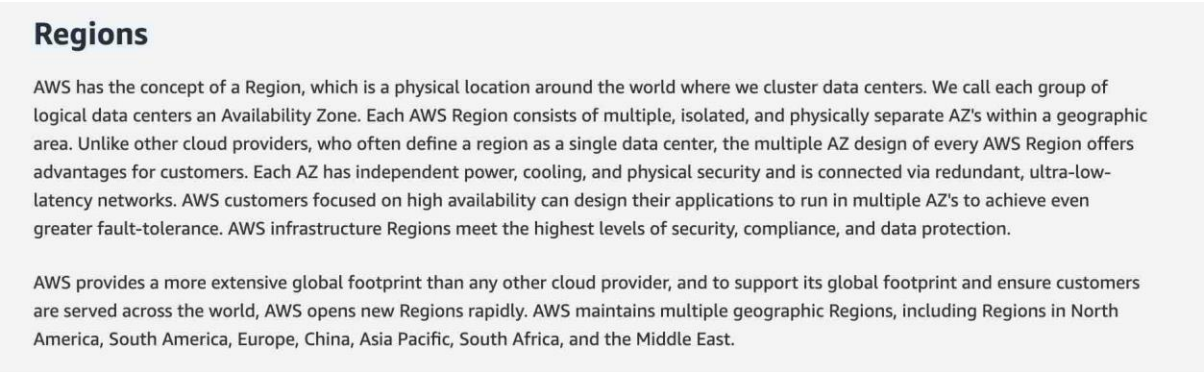
Question 43: Correct
Which of the following is best-suited for load-balancing HTTP and HTTPS traffic?

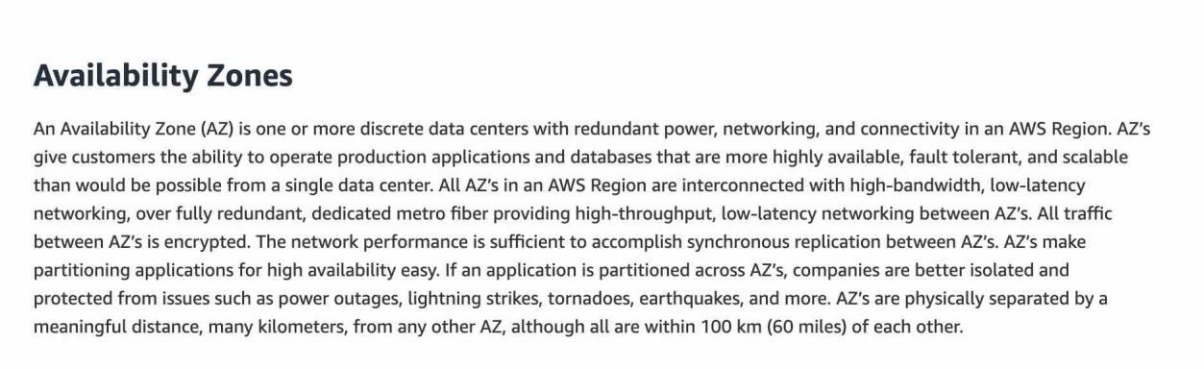
- Network Load Balancer
- AWS Auto Scaling
- Application Load Balancer **(Correct)**
- System Load Balancer

Explanation
Correct option:

Application Load Balancer

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault-tolerant.





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

Application Load Balancer is used for load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers.

Incorrect options:

Network Load Balancer - Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required.

AWS Auto Scaling - 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. Auto Scaling cannot be used for load-balancing HTTP and HTTPS traffic.

System Load Balancer - This is a made-up option and has been added as a distractor.

Reference:

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

Question 44: Correct
A financial services company wants to migrate from its on-premises data center to AWS Cloud. As a Cloud Practitioner, which AWS service would you recommend so that the company can compare the cost of running their IT infrastructure on-premises vs AWS Cloud?

- AWS Budgets
- AWS Total Cost of Ownership (TCO) Calculator **(Correct)**
- AWS Simple Monthly Calculator
- AWS Cost Explorer

Explanation
Correct option:

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. TCO calculator can be used from https://awstcocalculator.com/.

Incorrect options:

AWS Simple Monthly Calculator - The Simple Monthly Calculator helps customers and prospects estimate their monthly AWS bill more efficiently. The Simple Monthly Calculator cannot be used to compare the cost of running the IT infrastructure on-premises vs AWS Cloud.

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 be used to compare the cost of running the IT infrastructure on-premises vs AWS Cloud.

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 be used to compare the cost of running the IT infrastructure on-premises vs AWS Cloud.

Reference:

https://awstcocalculator.com/

Question 45: Correct
Which of the following can you use to run a bootstrap script while launching an EC2 instance?

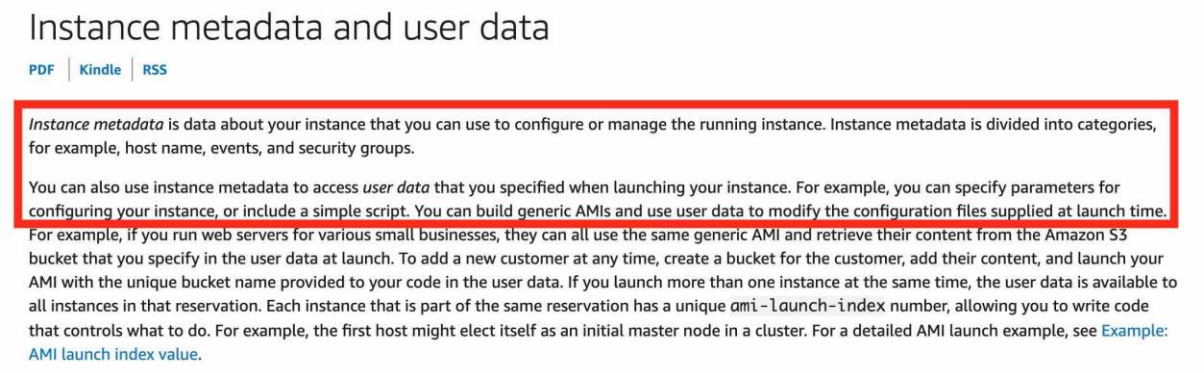
- EC2 instance AMI data
- EC2 instance configuration data
- EC2 instance metadata
- EC2 instance user data **(Correct)**

Explanation
Correct option:

EC2 instance user data

EC2 instance user data is the data that you specified in the form of a bootstrap script or configuration parameters while launching your instance.

EC2 instance metadata and user data:


Instance metadata and user data

PDF | Kindle | RSS

Instance metadata is data about your instance that you can use to configure or manage the running instance. Instance metadata is divided into categories, for example, host name, events, and security groups.

You can also use instance metadata to access *user data* that you specified when launching your instance. For example, you can specify parameters for configuring your instance, or include a simple script. You can build generic AMIs and use user data to modify the configuration files supplied at launch time. For example, if you run web servers for various small businesses, they can all use the same generic AMI and retrieve their content from the Amazon S3 bucket that you specify in the user data at launch. To add a new customer at any time, create a bucket for the customer, add their content, and launch your AMI with the unique bucket name provided to your code in the user data. If you launch more than one instance at the same time, the user data is available to all instances in that reservation. Each instance that is part of the same reservation has a unique `ami-launch-index` number, allowing you to write code that controls what to do. For example, the first host might elect itself as an initial master node in a cluster. For a detailed AMI launch example, see Example: AMI launch index value.

Incorrect options:

EC2 instance metadata - EC2 instance metadata is data about your instance that you can use to manage the instance. You can get instance items such as ami-id, public-hostname, local-hostname, hostname, public-ipv4, local-ipv4, public-keys, instance-id by using instance metadata. You cannot use EC2 instance metadata to run a bootstrap script while launching an EC2 instance. So this option is incorrect.

EC2 instance configuration data

EC2 instance AMI data

There is no such thing as EC2 instance configuration data or EC2 instance AMI data. These options have been added as distractors.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

Question 46: Correct
Which AWS service would you choose for a data processing project to store unstructured data?

- Amazon Aurora
- Amazon RDS
- Amazon RedShift
- Amazon DynamoDB **(Correct)**

Explanation
Correct option:

Amazon 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. DynamoDB offers flexible schema and can easily handle unstructured data.

Incorrect options:

Amazon RedShift - Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for large scale data set storage and analysis. Amazon Redshift does not support storing unstructured data.

Amazon Aurora - Amazon Aurora is an AWS service for relational databases. Aurora does not support storing unstructured data.

Amazon RDS - Amazon RDS is an AWS service for relational databases. RDS does not support storing unstructured data.

Reference:

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

Question 47: Incorrect

Which of the following are recommended security best practices for the AWS account root user? (Select two)

- [ ] Set up an IAM user with administrator permissions and do not use AWS account root user for administrative tasks
  (Correct)
- [ ] Disable MFA for the AWS account root user as it can lock the entire AWS account if the MFA device is lost
- [x] Enable MFA for the AWS account root user
  (Correct)
- [ ] Share AWS account root user access keys with other administrators
- [x] Keep your AWS account root user access keys in an encrypted file on S3
  (Incorrect)

Explanation
Correct options:

Enable MFA for the AWS account root user

Set up an IAM user with administrator permissions and do not use AWS account root user for administrative tasks

When you create an AWS account, you create an AWS account root user identity, which you use to sign in to AWS. You can sign in to the AWS Management Console using this root user identity—that is, the email address and password that you provided when creating the account. This combination of your email address and password is also called your root user credentials.

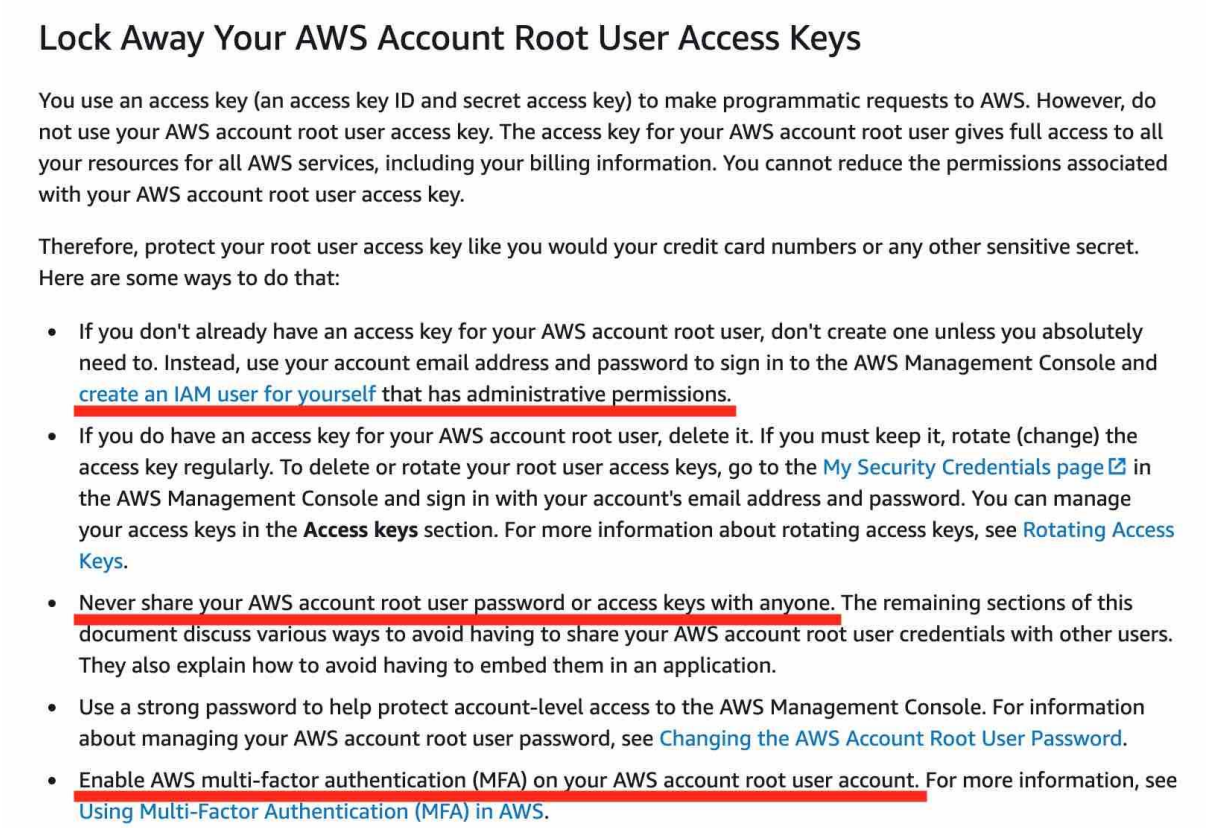
Some of the AWS account root user security best practices are as follows:

Do not use the AWS account root user for any task where it's not required. Instead, create a new IAM user for each person that requires administrator access. Then make those users administrators by placing the users into an "Administrators" group to which you attach the AdministratorAccess managed policy.

If you don't already have an access key for your AWS account root user, don't create one unless you need to. If you do have an access key for your AWS account root user, delete it.

Never share your AWS account root user password or access keys with anyone. Use a strong password to help protect account-level access to the AWS Management Console.

Enable AWS multi-factor authentication (MFA) on your AWS account root user account.



Lock Away Your AWS Account Root User Access Keys

You use an access key (an access key ID and secret access key) to make programmatic requests to AWS. However, do not use your AWS account root user access key. 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.

Therefore, protect your root user access key like you would your credit card numbers or any other sensitive secret. Here are some ways to do that:

- If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. Instead, use your account email address and password to sign in to the AWS Management Console and create an IAM user for yourself that has administrative permissions.
- If you do have an access key for your AWS account root user, delete it. If you must keep it, rotate (change) the access key regularly. To delete or rotate your root user access keys, go to the My Security Credentials page in the AWS Management Console and sign in with your account's email address and password. You can manage your access keys in the **Access keys** section. For more information about rotating access keys, see Rotating Access Keys.
- Never share your AWS account root user password or access keys with anyone. The remaining sections of this document discuss various ways to avoid having to share your AWS account root user credentials with other users. They also explain how to avoid having to embed them in an application.
- Use a strong password to help protect account-level access to the AWS Management Console. For information about managing your AWS account root user password, see Changing the AWS Account Root User Password.
- Enable AWS multi-factor authentication (MFA) on your AWS account root user account. For more information, see Using Multi-Factor Authentication (MFA) in AWS.

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

Incorrect options:

Disable MFA for the AWS account root user as it can lock the entire AWS account if the MFA device is lost - AWS recommends that you enable AWS multi-factor authentication (MFA) on your AWS account root user account.

Keep your AWS account root user access keys in an encrypted file on S3 - AWS recommends that if you do have an access key for your AWS account root user, delete it.

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.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials

https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html

Question 48: Correct

A financial services company wants to ensure that all customer data uploaded on its data lake on Amazon S3 always stays private. Which of the following is the MOST efficient solution to address this compliance requirement?

- Set up a high-level advisory committee to review the privacy settings of each object uploaded into S3
- Trigger a lambda function every time an object is uploaded on S3. The lambda function should change the object settings to make sure it stays private
- Use CloudWatch to ensure that all S3 resources stay private
- Use Amazon S3 Block Public Access to ensure that all S3 resources stay private **(Correct)**

Explanation
Correct option:

Use Amazon S3 Block Public Access to ensure that all S3 resources stay private

The Amazon S3 Block Public Access feature provides settings for access points, buckets, and accounts to help you manage public access to Amazon S3 resources. By default, new buckets, access points, and objects don't allow public access. However, users can modify bucket policies, access point policies, or object permissions to allow public access. S3 Block Public Access settings override these policies and permissions so that you can limit public access to these resources.

When Amazon S3 receives a request to access a bucket or an object, it determines whether the bucket or the bucket owner's account has a block public access setting applied. If the request was made through an access point, Amazon S3 also checks for block public access settings for the access point. If there is an existing block public access setting that prohibits the requested access, Amazon S3 rejects the request.

Amazon S3 Block Public Access
Overview:

Using Amazon S3 block public access

PDF | Kindle | RSS

The Amazon S3 Block Public Access feature provides settings for access points, buckets, and accounts to help you manage public access to Amazon S3 resources. By default, new buckets, access points, and objects don't allow public access. However, users can modify bucket policies, access point policies, or object permissions to allow public access. S3 Block Public Access settings override these policies and permissions so that you can limit public access to these resources.

With S3 Block Public Access, account administrators and bucket owners can easily set up centralized controls to limit public access to their Amazon S3 resources that are enforced regardless of how the resources are created.

When Amazon S3 receives a request to access a bucket or an object, it determines whether the bucket or the bucket owner's account has a block public access setting applied. If the request was made through an access point, Amazon S3 also checks for block public access settings for the access point. If there is an existing block public access setting that prohibits the requested access, Amazon S3 rejects the request.

Amazon S3 Block Public Access provides four settings. These settings are independent and can be used in any combination. Each setting can be applied to an access point, a bucket, or an entire AWS account. If the block public access settings for the access point, bucket, or account differ, then Amazon S3 applies the most restrictive combination of the access point, bucket, and account settings.

When Amazon S3 evaluates whether an operation is prohibited by a block public access setting, it rejects any request that violates an access point, bucket, or account setting.

Warning

Public access is granted to buckets and objects through access control lists (ACLs), access point policies, bucket policies, or all. To help ensure that all of your Amazon S3 access points, buckets, and objects have their public access blocked, we recommend that you turn on all four settings for block public access for your account. These settings block public access for all current and future buckets and access points.

Before applying these settings, verify that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, for example to host a static website as described at Hosting a static website on Amazon S3, you can customize the individual settings to suit your storage use cases.

via - https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-block-public-access.html

Incorrect options:

Trigger a lambda function every time an object is uploaded on S3. The lambda function should change the object settings to make sure it stays private - Although it's possible to implement this solution, but it is more efficient to use the "Amazon S3 Block Public Access" feature as its available off-the-shelf.

Use CloudWatch to ensure that all S3 resources stay private - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot be used to ensure data privacy on S3.

Set up a high-level advisory committee to review the privacy settings of each object uploaded into S3 - This option has been added as a distractor.

Reference:

https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-block-public-access.html

Question 49: Correct
Which of the following AWS services can be used to forecast your AWS account usage and costs?

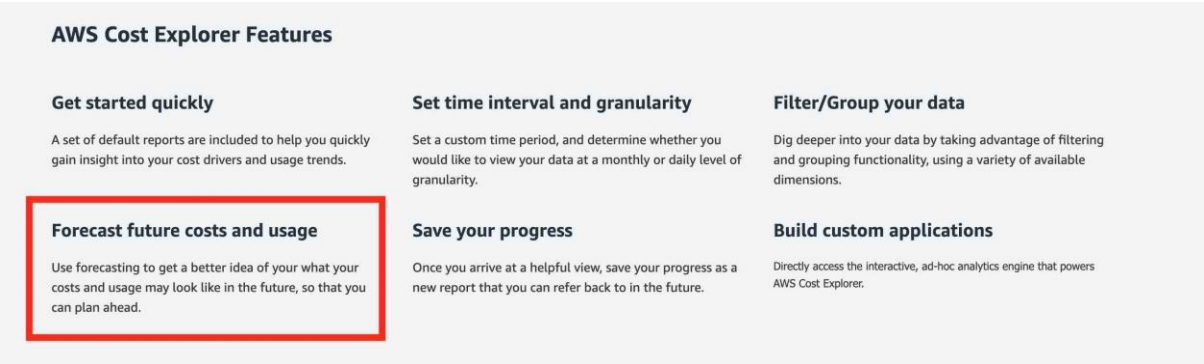
- AWS Cost and Usage Reports
- AWS Simple Monthly Calculator
- AWS Budgets
- AWS Cost Explorer **(Correct)**

Explanation
Correct 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. AWS Cost Explorer also supports forecasting to get a better idea of what your costs and usage may look like in the future so that you can plan.

AWS Cost Explorer
Features:



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

Incorrect options:

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 a comma-separated value (CSV) format. AWS Cost and Usage Reports cannot forecast your AWS account cost and usage.

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 forecast your AWS account cost and usage.

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. Simple Monthly Calculator cannot forecast your AWS account cost and usage.

Reference:

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

Question 50: Correct
Which of the following AWS authentication mechanisms supports a Multi-Factor Authentication (MFA) device that you can plug into a USB port on your computer?

- SMS text message-based MFA
- Virtual MFA device
- U2F security key **(Correct)**
- Hardware MFA device

Explanation
Correct option:

U2F security key - Universal 2nd Factor (U2F) Security Key is a device that you can 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.

How to enable the U2F Security Key for your own IAM user:

To enable a U2F security key for your own IAM user (console)

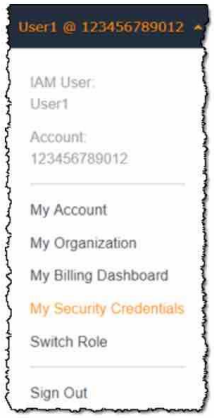
1. Use your AWS account ID or account alias, your IAM user name, and your password to sign in to the IAM console.

   Note

   For your convenience, the AWS sign-in page uses a browser cookie to remember your IAM user name and account information. If you previously signed in as a different user, choose **Sign in to a different account** near the bottom of the page to return to the main sign-in page. From there, you can type your AWS account ID or account alias to be redirected to the IAM user sign-in page for your account.

   To get your AWS account ID, contact your administrator.

2. In the navigation bar on the upper right, choose your user name, and then choose **My Security Credentials**.



3. On the **AWS IAM credentials** tab, in the **Multi-factor authentication** section, choose **Manage MFA device**.
4. In the **Manage MFA device** wizard, choose **U2F security key**, and then choose **Continue**.
5. Insert the U2F security key into your computer's USB port.

6. Tap the U2F security key, and then choose **Close** when U2F setup is complete.

via
- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_u2f.html

Incorrect options:

Virtual MFA device - This is 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.

Hardware MFA device - This is 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.

SMS text message-based MFA - This is a type of MFA in which the IAM user settings include the phone number of the user's SMS-compatible mobile device. When the user signs

in, AWS sends a six-digit numeric code by SMS text message to the user's mobile device. The user is required to type that code on a second webpage during sign-in.

References:

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

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_u2f.html

Question 51: Correct
Which AWS services can be used together to send alerts whenever the AWS account root user signs in? (Select two)

- ☐ Step Function
- ☐ SQS
- ☐ Lambda
- ☑ SNS **(Correct)**
- ☑ CloudWatch **(Correct)**

Explanation
Correct options:

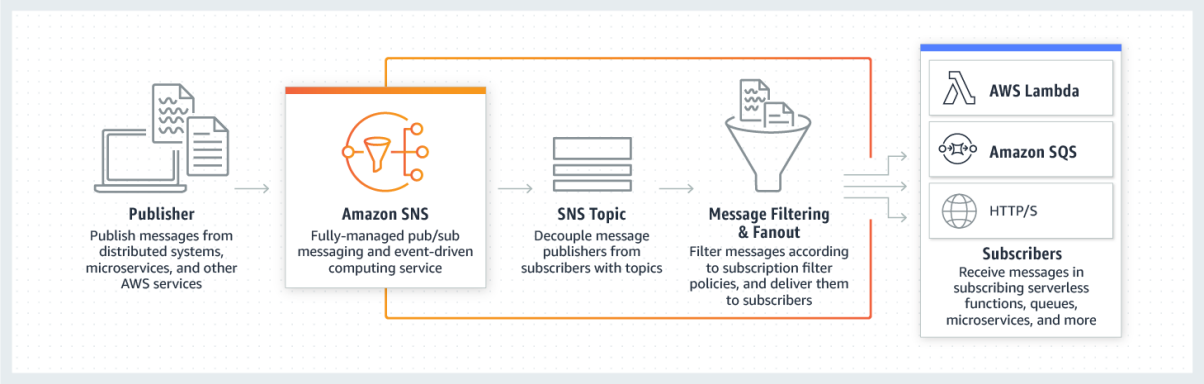
SNS

CloudWatch

Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams. CloudWatch Events becomes aware of operational changes as they occur. CloudWatch Events responds to these operational changes and takes corrective action as necessary, by sending messages to respond to the environment, activating functions, making changes, and capturing state information.

Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

How SNS
Works:



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

To send alerts whenever the AWS account root user signs in, you can create an Amazon Simple Notification Service (Amazon SNS) topic. Then, create an Amazon CloudWatch event rule to monitor userIdentity root logins from the AWS Management Console and send an email via SNS when the event triggers.

Incorrect options:

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.

Lambda - AWS Lambda is a compute service that lets you run code without provisioning or managing servers.

Step Function - AWS Step Function lets you coordinate multiple AWS services into serverless workflows. You can design and run workflows that stitch together services such as AWS Lambda, AWS Glue and Amazon SageMaker.

References:

https://aws.amazon.com/premiumsupport/knowledge-center/root-user-account-cloudwatch-rule/

https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html

Question 52: Correct
As per the Shared Responsibility Model, Security and Compliance is a shared responsibility between AWS and the customer. Which of the following security services falls under the purview of AWS under the Shared Responsibility Model?

- AWS Shield Advanced
- AWS Web Application Firewall (WAF)

- AWS Shield Standard
  (Correct)
- Security Groups for Amazon EC2

Explanation
Correct option:

AWS Shield Standard

AWS Shield is a managed service that protects against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is enabled for all AWS customers at no additional cost. AWS Shield Standard automatically protects your web applications running on AWS against the most common, frequently occurring DDoS attacks. You can get the full benefits of AWS Shield Standard by following the best practices of DDoS resiliency on AWS. As Shield Standard is automatically activated for all AWS customers with no options for any customizations, therefore AWS needs to manage the maintenance and configurations for this service. Hence this service falls under the purview of AWS.

Incorrect options:

AWS Web Application Firewall (WAF) - AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. AWS WAF has to be enabled by the customer and comes under the customer's responsibility.

AWS Shield Advanced - For higher levels of protection against attacks, you can subscribe to AWS Shield Advanced. As an AWS Shield Advanced customer, you can contact a 24x7 DDoS response team (DRT) for assistance during a DDoS attack. You also have exclusive access to advanced, real-time metrics and reports for extensive visibility into attacks on your AWS resources. Customers need to subscribe to Shield Advanced and need to pay for this service. It falls under customer responsibility per the AWS Shared Responsibility Model.

Security Groups for Amazon EC2 - A Security Group acts as a virtual firewall for the EC2 instance to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance. Security groups are the responsibility of the customer.

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

Question 53: **Correct**
Which of the following statements are true regarding Amazon Simple Storage Service (S3) (Select two)?

- S3 is a key value based object storage service
  (Correct)

- [x] S3 stores data in a flat non-hierarchical structure
  (Correct)
- [ ] You can install databases on S3
- [ ] S3 is a block storage service designed for a broad range of workloads
- [ ] S3 is a fully managed, elastic file system storage service used as database backup

Explanation
Correct options:

S3 is a key value based object storage service

S3 stores data in a flat non-hierarchical structure

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 stores data in a flat non-hierarchical structure. All objects are stored in S3 buckets and can be organized with shared names called prefixes. You can also append up to 10 key-value pairs called S3 object tags to each object, which can be created, updated, and deleted throughout an object's lifecycle.

Incorrect options:

S3 is a block storage service designed for a broad range of workloads - Block storage service is provided by Amazon Elastic Block Store (EBS) to provide persistent block-level storage volumes for use with Amazon EC2 instances. S3 is an object storage service.

S3 is a fully managed, elastic file system storage service used as database backup - 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. S3 is an object storage service.

You can install databases on S3 - S3 is an object storage service. You cannot install databases on S3.

Reference:

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

Question 54: **Correct**
Which AWS Route 53 routing policy would you use to route traffic to a single resource such as a web server for your website?

- Weighted routing policy
-

Latency routing policy

- Failover routing policy
- Simple routing policy **(Correct)**

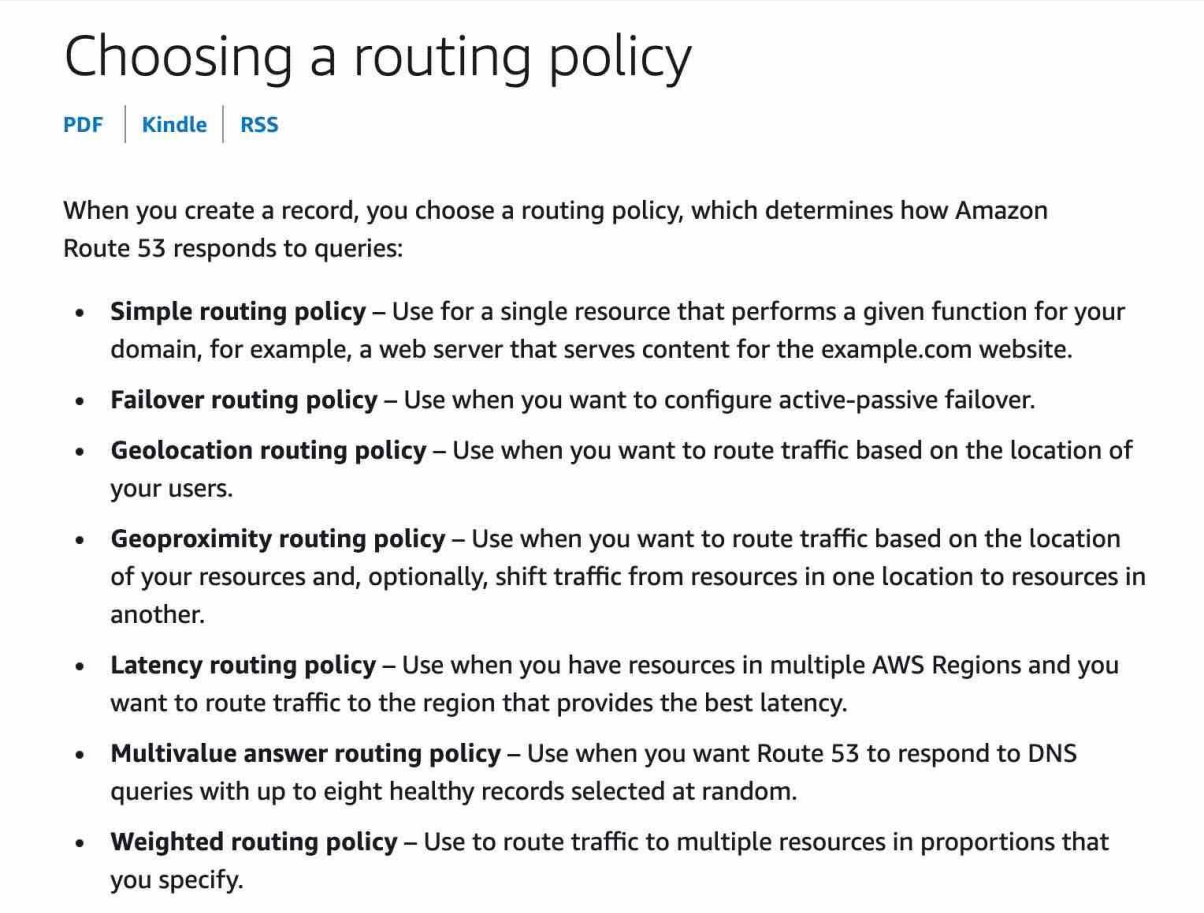
Explanation
Correct option:

Simple 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.

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.

Route 53 Routing Policy
Overview:



Choosing a routing policy

PDF | Kindle | RSS

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

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

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

Incorrect options:

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

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 55: **Incorrect**
Which of the following AWS Support plans provide programmatic access to AWS Support Center features to create, manage and close your support cases? (Select two)

- ☐ Basic
- ☐ Enterprise **(Correct)**
- ☐ Corporate
- ☑ Developer **(Incorrect)**
- ☑ Business **(Correct)**

Explanation
Correct 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. You get programmatic access (API Access) to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status.

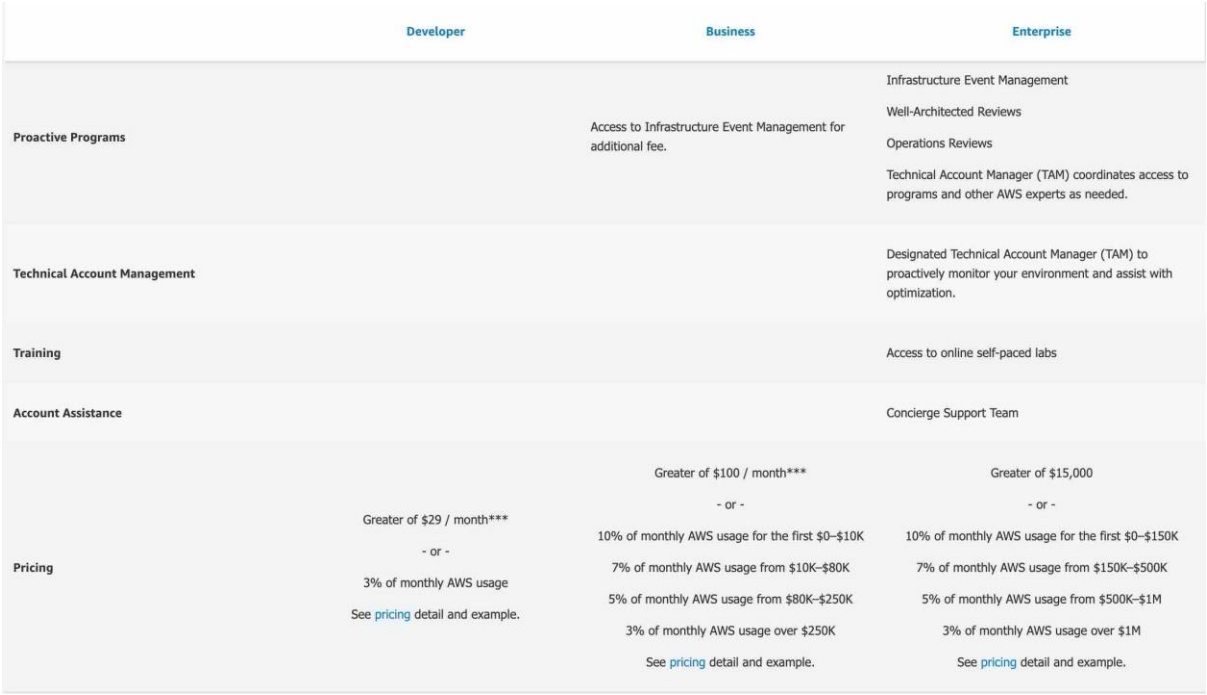
Business - AWS recommends Business Support if you have production workloads on AWS and want 24x7 phone, email and chat access to technical support and architectural guidance in the context of your specific use-cases. You get full access to AWS Trusted Advisor Best

Practice Checks. You get programmatic access (API Access) to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status.

Exam Alert:

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

	Developer	Business	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Recommended if you have production workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
AWS Trusted Advisor Best Practice Checks	7 Core checks	Full set of checks	Full set of checks
Enhanced Technical Support	Business hours** email access to Cloud Support Associates Unlimited cases / 1 primary contact	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported)
Case Severity / Response Times*	General guidance: < 24 business hours** System impaired: < 12 business hours**	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting



	Developer	Business	Enterprise
Proactive Programs		Access to Infrastructure Event Management for additional fee.	Infrastructure Event Management Well-Architected Reviews Operations Reviews Technical Account Manager (TAM) coordinates access to programs and other AWS experts as needed.
Technical Account Management			Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization.
Training			Access to online self-paced labs
Account Assistance			Concierge Support Team
Pricing	Greater of $29 / month*** - or - 3% of monthly AWS usage See pricing detail and example.	Greater of $100 / month*** - or - 10% of monthly AWS usage for the first $0–$10K 7% of monthly AWS usage from $10K–$80K 5% of monthly AWS usage from $80K–$250K 3% of monthly AWS usage over $250K See pricing detail and example.	Greater of $15,000 - or - 10% of monthly AWS usage for the first $0–$150K 7% of monthly AWS usage from $150K–$500K 5% of monthly AWS usage from $500K–$1M 3% of monthly AWS usage over $1M See pricing detail and example.

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

Incorrect options:

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.

Developer - AWS recommends the Developer Support plan if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours. This plan also supports general guidance on how services can be used for various use cases, workloads, or applications. You do not get access to Infrastructure Event Management with this plan.

Both these plans do not support programmatic access (API Access) to AWS Support Center.

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

Reference:

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

Question 56: Correct
An organization maintains a separate Virtual Private Cloud (VPC) for each of its business units. Two units need to privately share data. Which is the most optimal way of privately sharing data between the two VPCs?

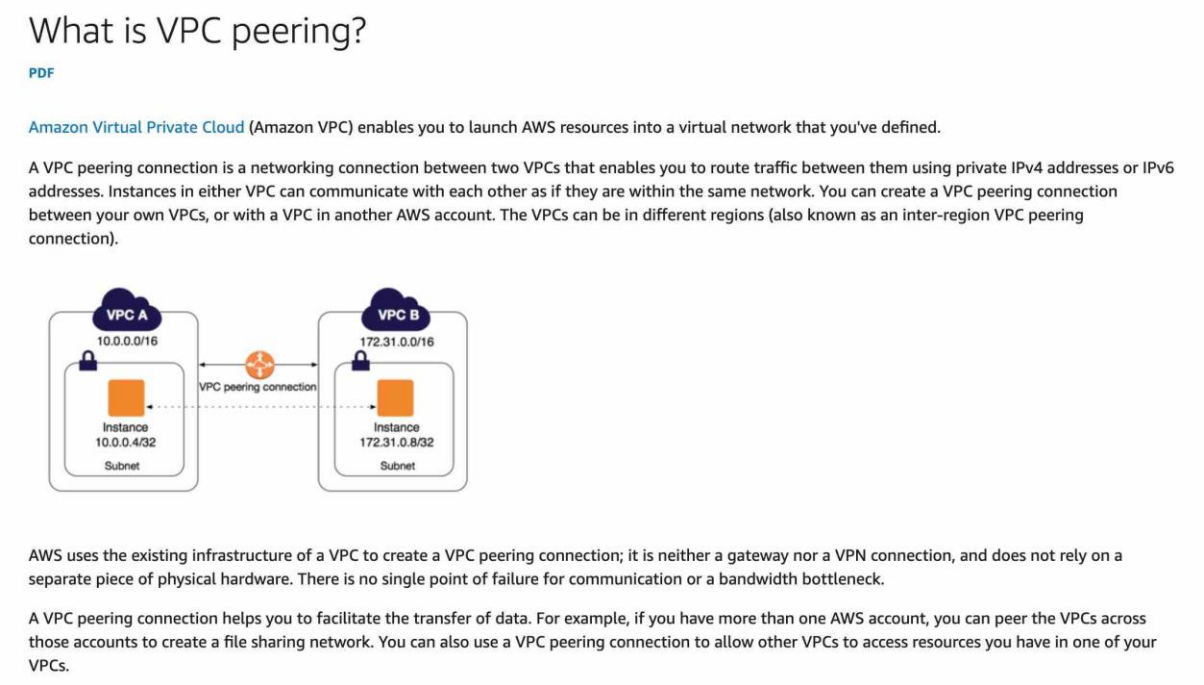
- VPC Peering **(Correct)**
- AWS Direct Connect
- Site to Site VPN
- VPC Endpoint

Explanation
Correct option:

VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

VPC Peering
Overview:



via - https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

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 cannot be used to interconnect VPCs.

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.

VPC Endpoint - A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. You cannot connect two VPCs using a VPC endpoint.

Reference:

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

Question 57: **Correct**
An e-commerce company would like to receive alerts when the Reserved EC2 Instances utilization drops below a certain threshold. Which AWS service can be used to address this use-case?

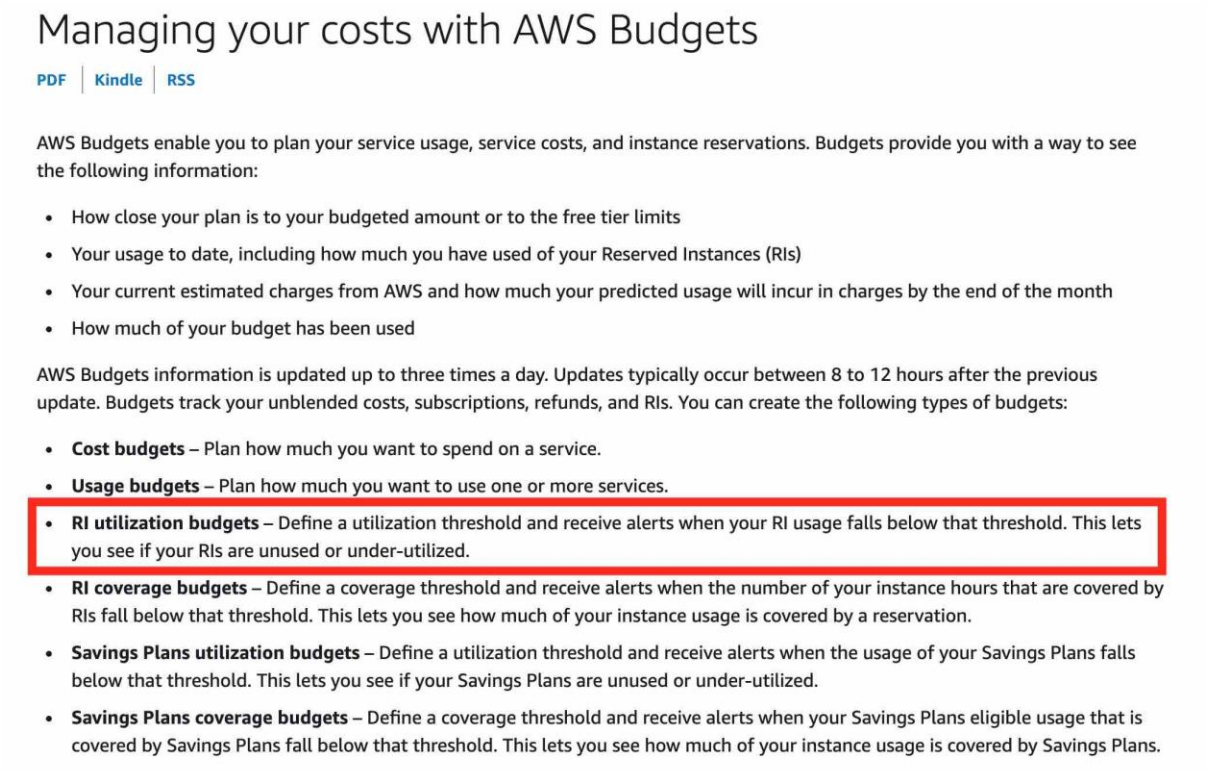
- AWS Trusted Advisor
- AWS Cost Explorer
- AWS Systems Manager
- AWS Budgets **(Correct)**

Explanation
Correct option:

AWS Budgets

AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. You can define a utilization threshold and receive alerts when your RI usage falls below that threshold. This lets you see if your RIs are unused or under-utilized. Reservation alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon Elasticsearch reservations.

AWS Budgets
Overview:



Managing your costs with AWS Budgets

PDF | Kindle | RSS

AWS Budgets enable you to plan your service usage, service costs, and instance reservations. Budgets provide you with a way to see the following information:

- How close your plan is to your budgeted amount or to the free tier limits
- Your usage to date, including how much you have used of your Reserved Instances (RIs)
- Your current estimated charges from AWS and how much your predicted usage will incur in charges by the end of the month
- How much of your budget has been used

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. You can create the following types of budgets:

- **Cost budgets** – Plan how much you want to spend on a service.
- **Usage budgets** – Plan how much you want to use one or more services.
- **RI utilization budgets** – Define a utilization threshold and receive alerts when your RI usage falls below that threshold. This lets you see if your RIs are unused or under-utilized.
- **RI coverage budgets** – Define a coverage threshold and receive alerts when the number of your instance hours that are covered by RIs fall below that threshold. This lets you see how much of your instance usage is covered by a reservation.
- **Savings Plans utilization budgets** – Define a utilization threshold and receive alerts when the usage of your Savings Plans falls below that threshold. This lets you see if your Savings Plans are unused or under-utilized.
- **Savings Plans coverage budgets** – Define a coverage threshold and receive alerts when your Savings Plans eligible usage that is covered by Savings Plans fall below that threshold. This lets you see how much of your instance usage is covered by Savings Plans.

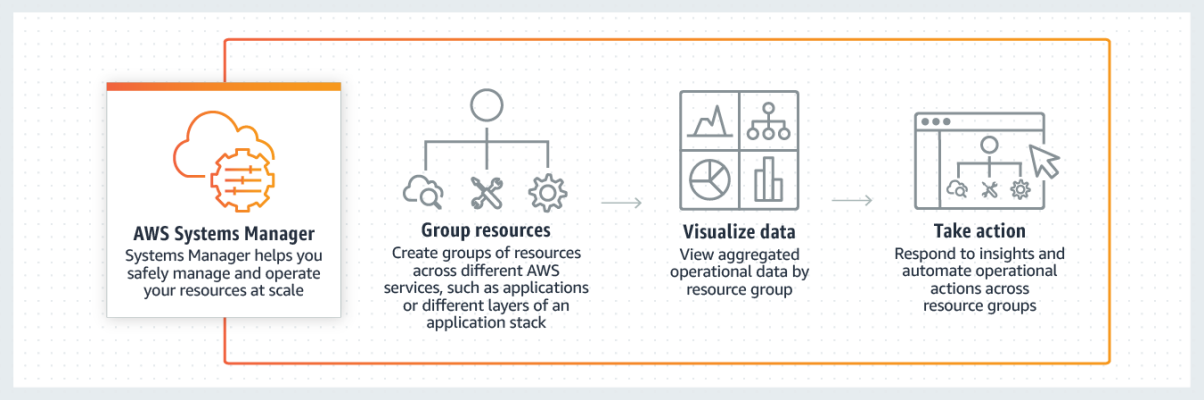
via - https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html

Incorrect options:

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 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 Systems Manager - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks such as running commands, managing patches, and configuring servers across AWS Cloud as well as on-premises infrastructure.



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

Reference:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html

Question 58: Correct
An e-commerce company wants to review the Payment Card Industry (PCI) reports on AWS Cloud. Which AWS resource can be used to address this use-case?

- AWS Secrets Manager
- AWS Cost and Usage Reports
- AWS Trusted Advisor
- AWS Artifact **(Correct)**

Explanation
Correct option:

AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to your organization. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. It is not a service, it's a no-cost, self-service portal for on-demand access to AWS' compliance reports.

Incorrect options:

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement,

recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally.

AWS Secrets Manager - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

AWS 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.

Reference:

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

Question 59: **Correct**
According to the AWS Shared Responsibility Model, which of the following are responsibilities of the customer for IAM? (Select two)

- ☐ Compliance validation for the underlying software infrastructure
- ☑ Analyze user access patterns and review IAM permissions **(Correct)**
- ☐ Configuration and vulnerability analysis for the underlying software infrastructure
- ☐ Manage global network security infrastructure
- ☑ Enable MFA on all accounts **(Correct)**

Explanation
Correct options:

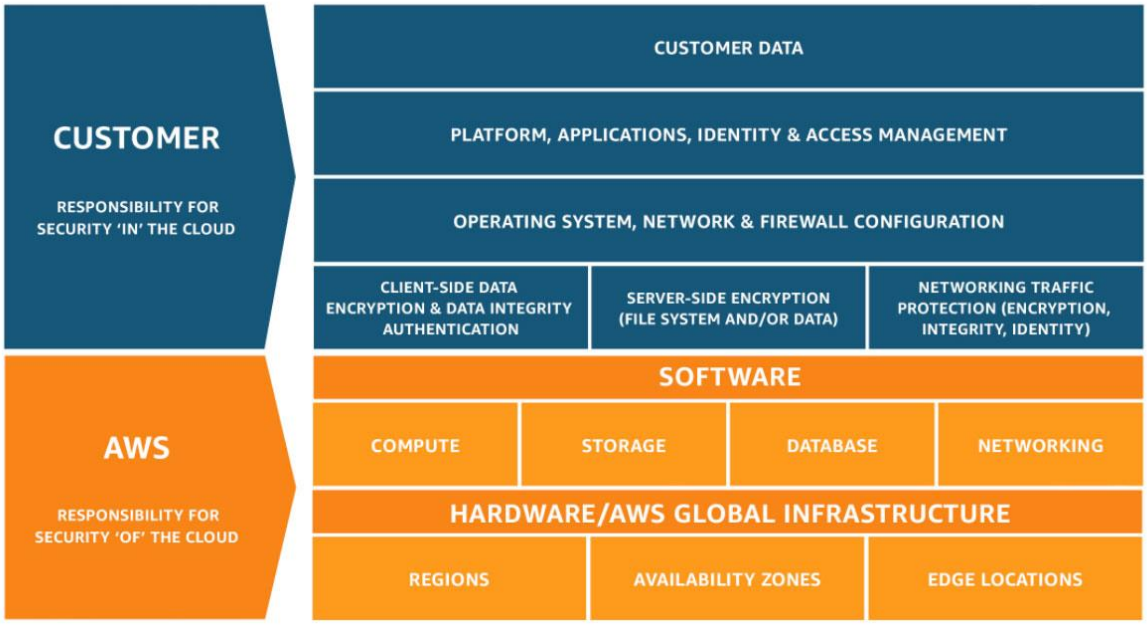
Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities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

Enable MFA on all accounts

Analyze user access patterns and review IAM permissions

Under the AWS Shared Responsibility Model, customers are responsible for enabling MFA on all accounts, analyzing access patterns and reviewing permissions.

Shared Responsibility Model
Overview:



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

Incorrect options:

Manage global network security infrastructure

Configuration and vulnerability analysis for the underlying software infrastructure

Compliance validation for the underlying software infrastructure

According to the AWS Shared Responsibility Model, AWS is responsible for "Security of the Cloud". This includes protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Therefore these three options fall under the responsibility of AWS.

Reference:

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

Question 60: Correct
Which of the following describes an Availability Zone in the AWS Cloud?

- One or more data centers in the same location **(Correct)**

One or more server racks in multiple locations

- One or more server racks in the same location

- One or more data centers in multiple locations

Explanation
Correct option:

"One or more data centers in the same location"

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:

"One or more data centers in multiple locations"

"One or more server racks in the same location"

"One or more server racks in multiple locations"

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

Reference:

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

Question 61: Correct
An e-commerce company has migrated its IT infrastructure from the on-premises data center to AWS Cloud. Which of the following costs is the company responsible for?

- Costs for hardware infrastructure on AWS Cloud
- Costs for powering servers on AWS Cloud
- Application software license costs **(Correct)**
- AWS Data Center physical security costs

Explanation
Correct option:

Application software license costs

Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the Internet with pay-as-you-go pricing. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Therefore, all costs for hardware infrastructure, powering servers and physical security for the Data Center fall under the ambit of AWS.

The customer needs to take care of software licensing costs and human resources costs.

Incorrect options:

AWS Data Center physical security costs

Costs for hardware infrastructure on AWS Cloud

Costs for powering servers on AWS Cloud

As per the details mentioned in the explanation above, these three options are not correct for the given use-case.

Reference:

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/what-is-cloud-computing.html

Question 62: Correct
Which AWS service can help you analyze your infrastructure to identify unattached or underutilized EBS volumes?

- AWS Config
- AWS Trusted Advisor **(Correct)**
- Amazon Inspector
- Amazon CloudWatch

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 can check Amazon Elastic Block Store (Amazon EBS) volume configurations and warns when volumes appear to be underused. Charges begin when a volume is created. If a volume remains unattached or has very low write activity (excluding boot volumes) for a period of time, the volume is probably not being used.

How Trusted Advisor
Works:

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

Incorrect options:

AWS Config - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. Think resource-specific change history, audit, and compliance; think Config. Its a configuration tracking service and not an infrastructure tracking service.

Amazon CloudWatch - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Amazon EBS emits notifications based on Amazon CloudWatch Events for a variety of volume, snapshot, and encryption status changes. With CloudWatch Events, you can establish rules that trigger programmatic actions in response to a change in volume, snapshot, or encryption key state (though not for underutilized volume usage).

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on your Amazon EC2 instances. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Its a security assessment service and not an infrastructure tracking service.

References:

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

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-cloud-watch-events.html

Question 63: Correct
A streaming media company wants to convert English language subtitles into Spanish language subtitles. As a Cloud Practitioner, which AWS service would you recommend for this use-case?

- Amazon Transcribe
- Amazon Translate **(Correct)**
- Amazon Rekognition
- Amazon Polly

Explanation
Correct option:

Amazon Translate

Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. Amazon Translate allows you to localize content - such as websites and applications - for international users, and to easily translate large volumes of text efficiently.

Incorrect options:

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

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

Amazon Rekognition - With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as to 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.

Reference:

https://aws.amazon.com/translate/

Question 64: **Correct**
Which of the following S3 storage classes has NO constraint of a minimum storage duration charge for objects?

- S3 Intelligent-Tiering
-

S3 One Zone-IA

- S3 Standard **(Correct)**
- S3 Glacier

Explanation
Correct option:

Correct options:

S3 Standard - S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. S3 Standard offers low latency and high throughput performance, It is designed for durability of 99.999999999% of objects across multiple Availability Zones. S3 Standard has no constraint of a minimum storage duration for objects.

Please review this illustration for S3 Storage Classes retrieval fee. You don't need to memorize the actual numbers, just remember that S3 Standard and S3 Intelligent-Tiering do not charge any retrieval
fee:

	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 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 Intelligent-Tiering mandates a minimum storage duration charge for 30 days.

S3 Glacier - Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. S3 Glacier mandates a minimum storage duration charge for 90 days.

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. S3 One Zone-IA mandates a minimum storage duration charge for 30 days.

Reference:

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

Question 65: **Incorrect**
Which AWS entity enables you to privately connect your VPC to an Amazon SQS queue?

- VPC Interface Endpoint **(Correct)**
- AWS Direct Connect
- Internet Gateway
- VPC Gateway Endpoint **(Incorrect)**

Explanation
Correct option:

VPC Interface Endpoint

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. AWS PrivateLink restricts all network traffic between your VPC and services to the Amazon network. You do not need an internet gateway, a NAT device, or a virtual private gateway.

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:

VPC Gateway Endpoint - 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. You cannot use VPC Gateway Endpoint to privately connect your VPC to an Amazon SQS queue.

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. You cannot use AWS Direct Connect to privately connect your VPC to an Amazon SQS queue.

Internet Gateway - An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. You cannot use an Internet Gateway to privately connect your VPC to an Amazon SQS queue.

Reference:

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