

Question 1:

How does AWS assist organisations' with their capacity requirements?

- ☒ With AWS you only pay for what you use
- ☐ You don't own the infrastructure
- ☒ You don't need to guess your capacity needs
(Correct)
- ☐ With AWS you don't pay for data centres

Explanation

All of these statements are true; however, the question is specifically asking how AWS can assist with capacity requirements.

i.e. how does AWS enable organizations to ensure they don't over or under-provision their resources.

The ability to scale on demand is the key advantage that can help them here as they can deploy what they know they need today and scale it as they need to tomorrow.

Question 2:

An AWS customer wishes to purchase unused Amazon EC2 capacity at a discounted rate. Which pricing plan should they choose?

- ☐ On-Demand Instances
- ☐ Reserved Instances
- ☒ Dedicated Instances
- ☐ Spot Instances
(Correct)

Explanation

Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices. Spot instances are best suited to workloads that can accept disruption as instances may be terminated if the capacity needs to be reclaimed by AWS.

CORRECT: "Spot Instances" is the correct answer.

INCORRECT: "Reserved Instances" is incorrect. Reserved instances do not leverage unused capacity, they are based on locking in for a fixed term of 1 or 3 years.

INCORRECT: "On-Demand Instances" is incorrect. There are no discounts for on-demand instances.

INCORRECT: "Dedicated Instances" is incorrect. Dedicated Instances are Amazon EC2 instances that run in a VPC on hardware that's dedicated to a single customer

Question 3:

Which resource should a new user on AWS use to get help with deploying popular technologies based on AWS best practices, including architecture and deployment instructions?

- ☐ AWS CloudFormation
- ☒ AWS Quick Starts
(Correct)
- ☐ AWS Config
- ☐ AWS Artifact

Explanation

Quick Starts are built by Amazon Web Services (AWS) solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

Each Quick Start includes AWS CloudFormation templates that automate the deployment and a guide that discusses the architecture and provides step-by-step deployment instructions.

CORRECT: "AWS Quick Starts" is the correct answer.

INCORRECT: "AWS CloudFormation" is incorrect. CloudFormation is used to deploy infrastructure from templates, the Quick Starts use CloudFormation.

INCORRECT: "AWS Artifact" is incorrect. Artifact provides on-demand access to AWS security and compliance reports.

INCORRECT: "AWS Config" is incorrect. Config is a service used for compliance relating the configuration of AWS resources.

Question 4: **Correct**

A manager is planning to migrate applications to the AWS Cloud and needs to obtain AWS compliance reports.

How can these reports be generated?

- ☐ Contact the AWS Compliance team.
- ☐

- ☐ Download the reports from AWS Secrets Manager.
- ☐ Create a support ticket with AWS Support.
- ☒ Download the reports from AWS Artifact.
(Correct)

Explanation

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.

Reports available in AWS Artifact include 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.

Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

CORRECT: "Download the reports from AWS Artifact" is the correct answer.

INCORRECT: "Contact the AWS Compliance team" is incorrect. You do not need to contact anyone at AWS, you can simply download this information.

INCORRECT: "Download the reports from AWS Secrets Manager" is incorrect. AWS Secrets Manager is used for storing secrets such as database authentication credentials or license codes. It is not used for storing compliance reports.

INCORRECT: "Create a support ticket with AWS Support" is incorrect. You do not need to contact anyone at AWS, you can simply download this information.

Question 5: **Correct**

Which AWS service or feature can be used to capture information about inbound and outbound IP traffic on network interfaces in a VPC?

- ☐ VPC Endpoint
- ☐ AWS CloudTrail
- ☒ VPC Flow Logs
(Correct)
- ☐ Internet gateway

Explanation

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

Flow logs can help you with a number of tasks, such as:

- Diagnosing overly restrictive security group rules
- Monitoring the traffic that is reaching your instance
- Determining the direction of the traffic to and from the network interfaces

Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency. You can create or delete flow logs without any risk of impact to network performance.

CORRECT: "VPC Flow Logs" is the correct answer.

INCORRECT: "Internet gateway" is incorrect. An internet gateway is attached to a VPC and used for sending and receiving data from the internet.

INCORRECT: "AWS CloudTrail" is incorrect. CloudTrail is used for auditing API activity.

INCORRECT: "VPC Endpoint" is incorrect. VPC endpoints are used for connecting to public AWS services using private IP addresses.

Question 6:

Which AWS service allows you to connect to storage from on-premise servers using standard file protocols?

- ☐ Amazon EBS
- ☐ Amazon S3
- ☐ Amazon Glacier
- ☒ Amazon EFS
(Correct)

Explanation

EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. EFS filesystems are mounted using the NFS protocol (which is a file-level protocol).

Access to EFS file systems from on-premises servers can be enabled via Direct Connect or AWS VPN.

You mount an EFS file system on your on-premises Linux server using the standard Linux mount command for mounting a file system via the NFSv4.1 or NFSv5 protocol.

CORRECT: "Amazon EFS" is the correct answer.

INCORRECT: "Amazon S3" is incorrect. Amazon S3 is an object-level not file-level storage system.

INCORRECT: "Amazon EBS" is incorrect. Amazon Elastic Block Storage (EBS) is block-level storage that can only be accessed by EC2 instances from the same AZ as the EBS volume.

INCORRECT: "Amazon Glacier" is incorrect. Amazon Glacier is an archiving solution that is accessed through S3.

Question 7:

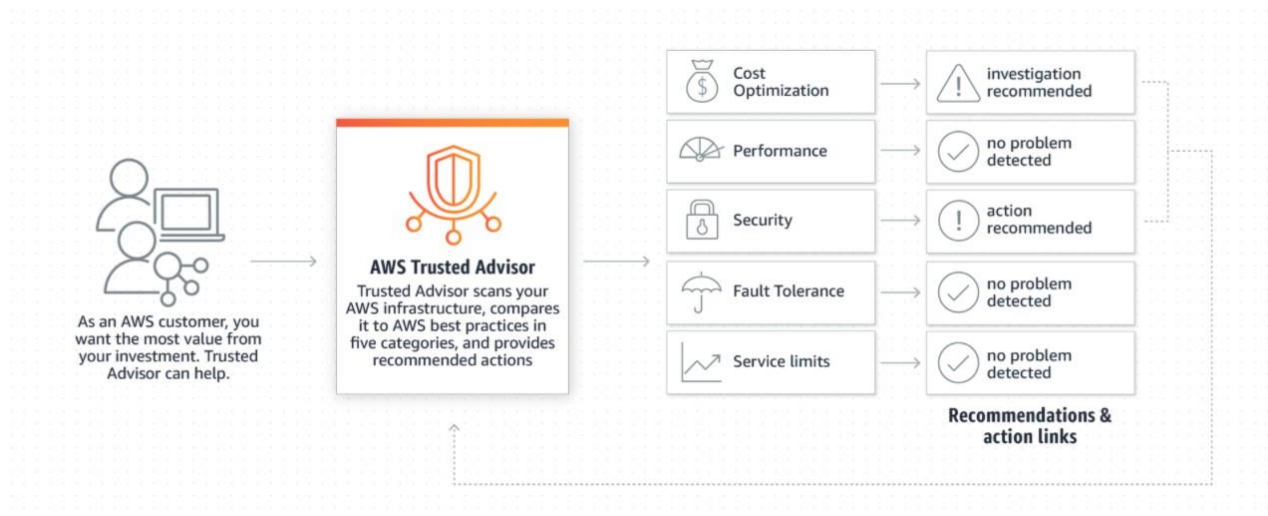
A user needs a quick way to determine if any Amazon EC2 instances have ports that allow unrestricted access.

Which AWS service will support this requirement?

- ☐ AWS Shield
- ☒ AWS Trusted Advisor
(Correct)
- ☐ AWS CloudWatch Logs
- ☐ VPC Flow Logs

Explanation

Access to the ports on an Amazon EC2 instance is controlled through security groups. AWS Trusted Advisor scans the security groups in your account to see if any security groups allow unrestricted access to any ports. This information is then presented to you in the console and you can then act on this information to secure the ports through editing the rules in the security group.



CORRECT: "AWS Trusted Advisor" is the correct answer.

INCORRECT: "VPC Flow Logs" is incorrect. VPC Flow Logs capture information about the IP traffic going to and from network interfaces in your VPC.

INCORRECT: "AWS Shield" is incorrect. AWS Shield is a managed service for mitigating distributed denial of service (DDoS) attacks.

INCORRECT: "AWS CloudWatch Logs" is incorrect. CloudWatch Logs captures logging information from applications and AWS services.

Question 8:

Which of the following is a method of backup available in the AWS cloud?

- ☐ Amazon EFS File Systems
- ☐ Availability Zones
- ☐ Amazon Route 53 Alias Record
- ☒ Amazon EBS Snapshots
(Correct)

Explanation

Amazon Elastic Block Store (EBS) is a block-based storage system that provides a “virtual hard disk in the cloud”. You can back up your EBS volumes using snapshots which are point-in-time copies of the data.

CORRECT: "Amazon EBS Snapshots" is the correct answer.

INCORRECT: "Availability Zones" is incorrect. Availability Zones are part of the AWS Global Infrastructure. AZs can be used for high availability and fault tolerance as you can architect your applications to be spread across them. However, they are not a backup solution.

INCORRECT: "Amazon EFS File Systems" is incorrect. The Amazon Elastic File System (EFS) provides file-based storage that you access using the NFS v2 protocol. This is storage service but not a backup service. You can backup EFS using the AWS Backup service or using EFS-to-EFS backup.

INCORRECT: "Amazon Route 53 Alias Record" is incorrect. Amazon Route 53 provides a DNS service and an Alias record is a type of record that can map a public domain name to an AWS service target.

Question 9:

A company plans to deploy a global commercial application on Amazon EC2 instances. The deployment solution should be designed with the highest redundancy and fault tolerance.

Based on this situation, how should the EC2 instances be deployed?

- ☐ In a single Availability Zone in two AWS Regions

- ☒ Across multiple Availability Zones in two AWS Regions
(Correct)
- ☐ Across multiple Availability Zones in one AWS Region
- ☐ In a single Availability Zone in one AWS Region

Explanation

For maximum redundancy and fault tolerance the application should be deployed in multiple AWS Regions and multiple Availability Zones within each of those regions. This architecture may use Elastic Load Balancers and Amazon Route 53 records to direct traffic to instances. Alternatively, it could use AWS Global Accelerator.

CORRECT: "Across multiple Availability Zones in two AWS Regions" is the correct answer.

INCORRECT: "In a single Availability Zone in one AWS Region" is incorrect as this does not represent the highest redundancy and fault tolerance.

INCORRECT: "In a single Availability Zone in two AWS Regions" is incorrect as this does not represent the highest redundancy and fault tolerance.

INCORRECT: "Across multiple Availability Zones in one AWS Region" is incorrect as this does not represent the highest redundancy and fault tolerance.

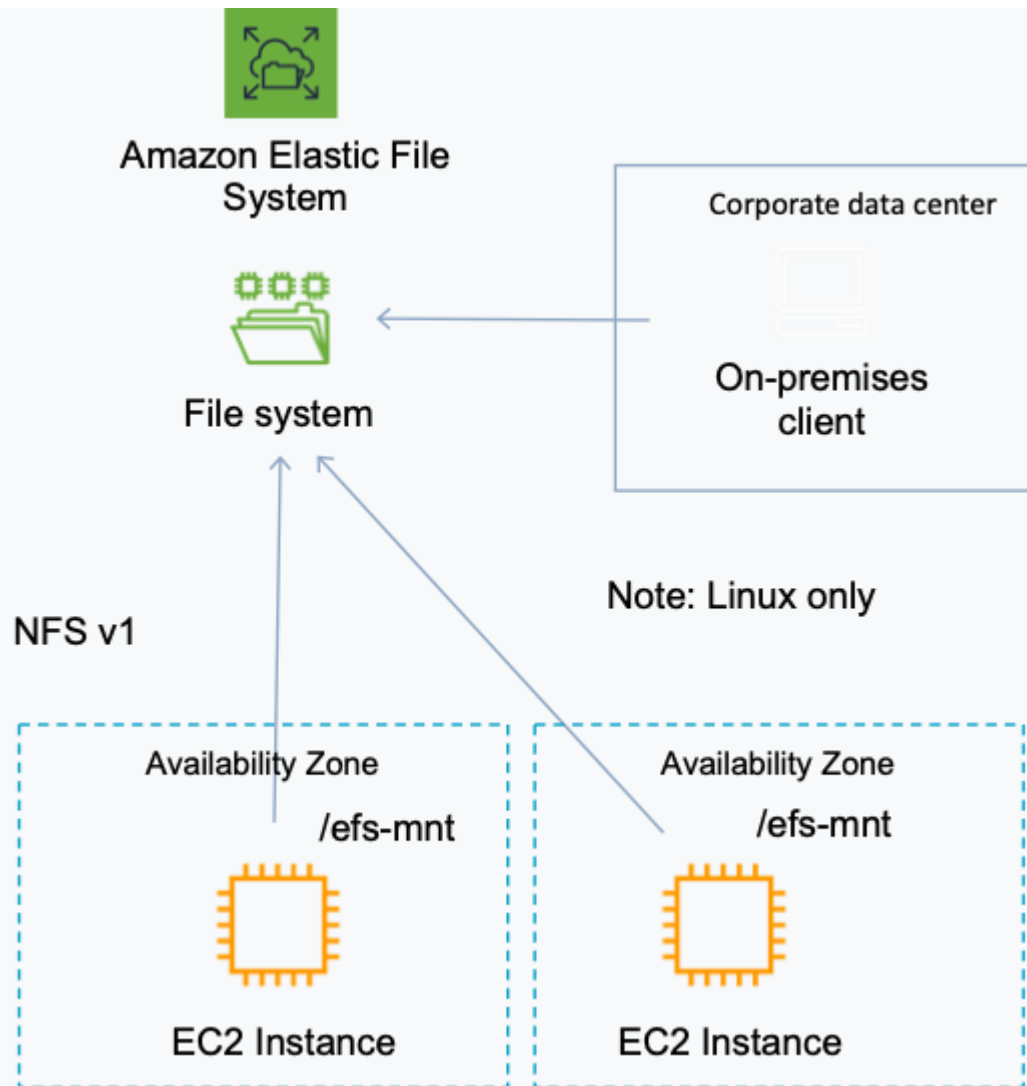
Question 10:

Which storage service allows you to connect multiple EC2 instances concurrently using file-level protocols?

- ☐ Amazon S3
- ☐ Amazon Glacier
- ☒ Amazon EFS
(Correct)
- ☐ Amazon EBS

Explanation

Amazon Elastic File System allows you to connect hundreds or thousands of EC2 instances concurrently and is accessed using the file-level NFS protocol.



CORRECT: "Amazon EFS" is the correct answer.

INCORRECT: "Amazon S3" is incorrect. Amazon S3 is an object storage system.

INCORRECT: "Amazon EBS" is incorrect. Amazon Elastic Block Storage provides block-level volumes to individual EC2 instances (cannot connect multiple instances to a single EBS volume)

INCORRECT: "Amazon Glacier" is incorrect. Glacier is used for archiving S3 objects.

Question 11:

What benefits are provided by Amazon CloudFront? (Select TWO.)

- ☐ Used to enable private subnet instances to access the Internet
- ☒ Content is cached at Edge Locations for fast distribution to customers
(Correct)
- ☐ Provides a worldwide distributed DNS service
- ☒ Built-in Distributed Denial of Service (DDoS) attack protection
(Correct)

- ☐ Allows you to register domain names

Explanation

CloudFront is a content delivery network (CDN) that allows you to store (cache) your content at “edge locations” located around the world. This allows customers to access content more quickly and provides security against DDoS attacks. CloudFront can be used for data, videos, applications, and APIs.

Benefits include:

- Cache content at Edge Location for fast distribution to customers.
- Built-in Distributed Denial of Service (DDoS) attack protection.
- Integrates with many AWS services (S3, EC2, ELB, Route 53, Lambda).

CORRECT: "Built-in Distributed Denial of Service (DDoS) attack protection" is a correct answer.

CORRECT: "Content is cached at Edge Locations for fast distribution to customers" is a correct answer.

INCORRECT: "Allows you to register domain names" is incorrect. Amazon Route 53 can be used for registering domain names.

INCORRECT: "Used to enable private subnet instances to access the Internet" is incorrect \$

INCORRECT: "Provides a worldwide distributed DNS service" is incorrect. Amazon Route 53 provides a worldwide distributed DNS service.

Question 12:

The AWS global infrastructure is composed of? (Select TWO.)

- ☐ Fault Zones
- ☒ IP Subnets
- ☐ Availability Zones
(Correct)
- ☐ Clusters
- ☒ Regions
(Correct)

Explanation

The AWS Global infrastructure is built around Regions and Availability Zones (AZs). A Region is a physical location in the world where AWS have multiple AZs. AZs consist of

one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities

CORRECT: "Regions" is a correct answer.

CORRECT: "Availability Zones" is also a correct answer.

INCORRECT: "Clusters" is incorrect as this is not part of the AWS global infrastructure.

INCORRECT: "Fault Zones" is incorrect as this is not part of the AWS global infrastructure.

INCORRECT: "IP subnets" is incorrect as this is not part of the AWS global infrastructure.

Question 13:

A company plans to connect their on-premises data center to the AWS Cloud and requires consistent bandwidth and performance.

Which AWS service should the company choose?

- ☐ AWS VPN
- ☐ Amazon CloudFront
- ☒ Amazon Connect
- ☐ AWS Direct Connect
(Correct)

Explanation

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.

CORRECT: "AWS Direct Connect" is the correct answer.

INCORRECT: "AWS VPN" is incorrect. A virtual private network (VPN) uses the internet and does not offer consistent network bandwidth or performance.

INCORRECT: "Amazon Connect" is incorrect. This is contact centre solution, not a networking technology.

INCORRECT: "Amazon CloudFront" is incorrect. CloudFront is a CDN used for caching content. It is not used for connecting from on-premises data centers to the AWS Cloud.

Question 14:

What advantages does a database administrator obtain by using the Amazon Relational Database Service (RDS)?

- ☒ RDS simplifies relational database administration tasks.
(Correct)
- ☐ RDS enables users to dynamically adjust CPU and RAM resources.
- ☐ RDS provides 99.9999999999% reliability and durability.
- ☐ RDS databases automatically scale based on load.

Explanation

Amazon RDS is a managed relational database service on which you can run several types of database software. The service is managed so this reduces the database administration tasks an administrator would normally undertake. The managed service includes hardware provisioning, database setup, patching and backups.

CORRECT: "RDS simplifies relational database administration tasks" is the correct answer.

INCORRECT: "RDS databases automatically scale based on load" is incorrect. This is not true, storage auto scaling is possible but for compute it scales by changing instance type (manual).

INCORRECT: "RDS provides 99.9999999999% reliability and durability" is incorrect. This is not true of Amazon RDS.

INCORRECT: "RDS enables users to dynamically adjust CPU and RAM resources" is incorrect. You cannot adjust CPU and RAM dynamically, you must change the instance type and reboot the database instance.

Question 15:

Which service can be used to track the CPU usage of an EC2 instance?

- ☐ Amazon CloudFormation
- ☐ Amazon CloudFront
- ☒ Amazon CloudWatch
(Correct)
- ☐ Amazon CloudTrail

Explanation

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. CloudWatch is for performance monitoring, whereas CloudTrail is for auditing

CORRECT: "Amazon CloudWatch" is the correct answer.

INCORRECT: "Amazon CloudTrail" is incorrect. AWS CloudTrail is a web service that records activity made on your account and delivers log files to an Amazon S3 bucket.

INCORRECT: "Amazon CloudFront" is incorrect. CloudFront is a content delivery network (CDN) that caches content.

INCORRECT: "Amazon CloudFormation" is incorrect. CloudFormation is used for automated provisioning of infrastructure.

Question 16:

Which AWS service can be used to convert video and audio files from their source format into versions that will playback on devices like smartphones, tablets and PC?

- ☐ Elastic Load Balancer
- ☐ Elastic Beanstalk
- ☒ Elastic Transcoder
(Correct)
- ☐ Auto Scaling

Explanation

Amazon Elastic Transcoder is a highly scalable, easy to use and cost-effective way for developers and businesses to convert (or "transcode") video and audio files from their source format into versions that will playback on devices like smartphones, tablets and PCs.

CORRECT: "Elastic Transcoder" is the correct answer.

INCORRECT: "Elastic Beanstalk" is incorrect. AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud.

INCORRECT: "Elastic Load Balancer" is incorrect. ELB is used to distribute incoming connections to EC2 instances

INCORRECT: "Auto Scaling" is incorrect. Auto Scaling is used to automatically ensure the right number of EC2 instances are available to service current load.

Question 17:

Which AWS service is primarily used for software version control?

- ☐ AWS CodeStar
- ☐ AWS CodeDeploy

- ☒ AWS CodeCommit
(Correct)
- ☐ AWS Cloud9

Explanation

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem.

CORRECT: "AWS CodeCommit" is the correct answer.

INCORRECT: "AWS CodeStar" is incorrect. AWS CodeStar enables you to quickly develop, build, and deploy applications on AWS. AWS CodeStar provides a unified user interface, enabling you to easily manage your software development activities in one place.

INCORRECT: "AWS Cloud9" is incorrect. AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser.

INCORRECT: "AWS CodeDeploy" is incorrect. AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda functions.

Question 18:

Which AWS service is used to enable multi-factor authentication?

- ☒ AWS IAM
(Correct)
- ☐ AWS KMS
- ☐ Amazon STS
- ☐ Amazon EC2

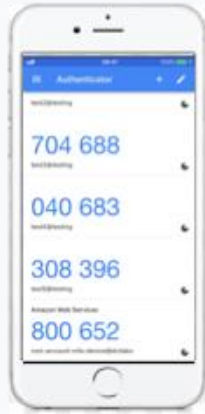
Explanation

The identity and access management service (IAM) is used to securely control individual and group access to AWS resources. IAM can also be used to manage multi-factor authentication (MFA). With MFA you add an additional factor of authentication such as Google Authenticator device. This is "something you have" and is used with your password "something you know".

Something you know:

EJPx!*21p9%
Password

Something you have:



Something you are:



CORRECT: "AWS IAM" is the correct answer.

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

INCORRECT: "Amazon EC2" is incorrect. Amazon EC2 is used for running operating systems instances in the cloud.

INCORRECT: "AWS KMS" is incorrect. AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.

Question 19:

Which tasks can a user complete using the AWS Cost Management tools? (Select TWO.)

- ☒ Automatically terminate AWS resources if budget thresholds are exceeded.
- ☐ Move data stored in Amazon S3 Standard to an archiving storage class to reduce cost.
- ☐ Break down AWS costs by day, service, and linked AWS account. **(Correct)**
- ☐ Launch either EC2 Spot instances or On-Demand instances based on the current pricing.
- ☒ Create budgets and receive notifications if current or forecasted usage exceeds the budgets. **(Correct)**

Explanation

The AWS Cost Management tools includes services, tools, and resources to organize and track cost and usage data, enhance control through consolidated billing and access

permissions, enable better planning through budgeting and forecasts, and further lower costs with resources and pricing optimizations.

CORRECT: "Break down AWS costs by day, service, and linked AWS account" is a correct answer.

CORRECT: "Create budgets and receive notifications if current or forecasted usage exceeds the budgets" is also a correct answer.

INCORRECT: "Automatically terminate AWS resources if budget thresholds are exceeded" is incorrect. The cost management tools will not do this for you but they could generate an alert which could be processed by another service to terminate resources.

INCORRECT: "Launch either EC2 Spot instances or On-Demand instances based on the current pricing" is incorrect. The cost management tools do not integrate with the tools used to launch EC2 instances and cannot choose the best pricing plan.

INCORRECT: "Move data stored in Amazon S3 Standard to an archiving storage class to reduce cost" is incorrect. This is performed using lifecycle management in Amazon S3, it is not a task performed by cost management tools.

Question 20:

Which services are involved in reducing application latency and increasing performance for end users? (Select TWO.)

- ☐ Amazon Workspaces
- ☒ Amazon CloudFront
(Correct)
- ☒ Amazon ElastiCache
(Correct)
- ☐ Amazon ECS
- ☐ Amazon S3

Explanation

Amazon ElastiCache is an in-memory cache that can be placed in front of databases such as Amazon RDS to cache queries for better performance. Amazon CloudFront is a content delivery network (CDN) service that caches media such as videos and photos in locations around the world for lower latency and improved performance.

CORRECT: "Amazon ElastiCache" is a correct answer.

CORRECT: "Amazon CloudFront" is a correct answer.

INCORRECT: "Amazon ECS" is incorrect. This service is used for running Docker containers on AWS. Its function is not primarily to improve performance.

INCORRECT: "Amazon S3" is incorrect. Amazon S3 is an object-based storage system. To improve performance of access to objects globally you would use CloudFront to cache the objects.

INCORRECT: "Amazon Workspaces" is incorrect. This service is used for running managed desktops in the cloud.

Question 21:

Which aspects of security on AWS are customer responsibilities? (Select TWO.)

- ☒ Setting up account password policies
(Correct)
- ☐ Physical access controls
- ☐ Patching of storage systems
- ☒ Server-side encryption
(Correct)
- ☐ Availability of AWS regions

Explanation

AWS are responsible for the "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.

The customer is responsible for "security in the cloud". Customer responsibility depends on the service consumed but includes aspects such as Identity and Access Management (includes password policies), encryption of data, protection of network traffic, and operating system, network and firewall configuration.

Question 22:

Which AWS service can be used to track the activity of users on AWS?

- ☐ Amazon CloudWatch
- ☒ AWS CloudTrail
(Correct)
- ☐ Amazon Inspector
- ☐ AWS Directory Service

Explanation

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

Think of CloudTrail is an auditing service (who did what and when), and CloudWatch as a performance monitoring service (how much resource was used).

CORRECT: "AWS CloudTrail" is the correct answer.

INCORRECT: "AWS Directory Service" is incorrect. This service provides several options for running directory services on AWS and connecting to directory services on-premises.

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

INCORRECT: "Amazon CloudWatch" is incorrect. CloudWatch is used for performance monitoring, not auditing.

Question 23:

A company recently took up an Enterprise-level AWS Support plan and has a question relating to their AWS account. Who is the primary point of contact they should direct the question to?

- ☒ AWS Partner Network (APN) partner
- ☐ AWS Solutions Architect
- ☒ AWS Concierge Support team
(Correct)
- ☐ Cloud Support Associates

Explanation

Customers on an Enterprise-level AWS Support plan should contact the AWS Concierge Support team for assistance related to their AWS account. The excerpt below from the support plans overview table shows that only enterprise plans can use the concierge support team:

	Developer	Business	Enterprise
Technical Account Management			Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization and coordinate access to programs and AWS experts
Training			Access to online self-paced labs
Account Assistance			Concierge Support Team

CORRECT: "AWS Concierge Support team" is the correct answer.

INCORRECT: "Cloud Support Associates" is incorrect. This team can be used by customers on the Developer plan for technical support in business hours by email.

INCORRECT: "AWS Solutions Architect" is incorrect. Solutions Architects are not provided for account questions.

INCORRECT: "AWS Partner Network (APN) partner" is incorrect. The APN is a global partner program for technology and consulting businesses who leverage Amazon Web Services to build solutions and services for customers.

Question 24:

Which AWS storage technology can be considered a "virtual hard disk in the cloud"?

- ☐ Amazon S3 object
- ☒ Amazon Elastic Block Storage (EBS) volume
(Correct)
- ☐ Amazon Elastic File Storage (EFS) filesystem
- ☐ Amazon Glacier archive

Explanation

An EBS volume is a block storage device that is most similar to a virtual hard disk in the cloud as when attached to an instance it appears as a local disk that can have an operating system installed on or be formatted and used for any other local storage purpose.

CORRECT: "Amazon Elastic Block Storage (EBS) volume" is the correct answer.

INCORRECT: "Amazon Elastic File Storage (EFS) filesystem" is incorrect. An EFS filesystem is mounted over the NFS protocol which is a file-level protocol. Therefore, it is a network filesystem not a virtual hard disk and cannot have an operating system installed or be formatted and used as a locally attached disk.

INCORRECT: "Amazon S3 object" is incorrect. S3 is an object storage system and cannot be mounted and used as a virtual hard drive.

INCORRECT: "Amazon Glacier archive" is incorrect. Glacier is an archiving solution where you can archive your S3 objects at extremely low cost.

Question 25:

Which of the following is a principle of good AWS Cloud architecture design?

- ☐ Implement monolithic design
- ☒ Implement loose coupling
(Correct)
- ☐ Implement vertical scaling
- ☐ Implement single points of failure

Explanation

As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components.

This means that IT systems should be designed in a way that reduces interdependencies—a change or a failure in one component should not cascade to other components.

CORRECT: "Implement loose coupling" is the correct answer.

INCORRECT: "Implement single points of failure" is incorrect. Single points of failure should be eliminated where possible to avoid system/application outages.

INCORRECT: "Implement monolithic design" is incorrect. Monolithic design is when multiple components are tightly coupled and this increases the impact of a system failure.

INCORRECT: "Implement vertical scaling" is incorrect. Vertical scaling means adding resources such as CPU and memory to an existing application or instance. Where possible horizontal scaling should be used with loose coupling.

Question 26:

A Cloud Practitioner requires point-in-time recovery (PITR) for an Amazon DynamoDB table. Who is responsible for configuring and performing backups?

- ☒ The customer is responsible for both tasks.
- ☐ AWS is responsible for configuring and the user is responsible for performing backups.
- ☐ AWS is responsible for both tasks.
- ☐ The customer is responsible for configuring and AWS is responsible for performing backups.
(Correct)

Explanation

Point-in-time recovery (PITR) provides continuous backups of your DynamoDB table data. When enabled, DynamoDB maintains incremental backups of your table for the last 35 days until you explicitly turn it off. It is a customer responsibility to enable PITR on and AWS is responsible for actually performing the backups.

CORRECT: "The customer is responsible for configuring and AWS is responsible for performing backups" is the correct answer.

INCORRECT: "AWS is responsible for configuring and the user is responsible for performing backups" is incorrect. This is backwards, users are responsible for configuring and AWS is responsible for performing backups.

INCORRECT: "AWS is responsible for both tasks" is incorrect. This is not true as users must configure PITR.

INCORRECT: "The customer is responsible for both tasks" is incorrect. This is not true, AWS perform the backups.

Question 27:

A company needs to publish messages to a thousands of subscribers simultaneously using a push mechanism.

Which AWS service should the company use?

- ☒ Amazon Simple Notification Service (Amazon SNS)
(Correct)
- ☐ Amazon Simple Queue Service (Amazon SQS)
- ☐ Amazon Simple Workflow Service (SWF)
- ☐ AWS Step Functions

Explanation

Amazon SNS is a publisher/subscriber notification service that uses a push mechanism to publish messages to multiple subscribers. Amazon SNS enables you to send messages or notifications directly to users with SMS text messages to over 200 countries, mobile push on Apple, Android, and other platforms or email (SMTP).

CORRECT: "Amazon Simple Notification Service (Amazon SNS)" is the correct answer.

INCORRECT: "Amazon Simple Queue Service (Amazon SQS)" is incorrect. SQS is a message queue service used for decoupling applications.

INCORRECT: "Amazon Simple Workflow Service (SWF)" is incorrect. SWF is a workflow orchestration service, not a messaging service.

INCORRECT: "AWS Step Functions" is incorrect. AWS Step Functions is a serverless workflow orchestration service for modern applications.

Question 28:

Which AWS service can an organization use to automate operational tasks on EC2 instances using existing Chef cookbooks?

- ☒ AWS OpsWorks
(Correct)
- ☐ AWS Config
- ☐ AWS Service Catalog
- ☐

Explanation

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. With Chef, you use code templates, or cookbooks, to describe the desired configuration of instances or on-premises server.

CORRECT: "AWS OpsWorks" is the correct answer.

INCORRECT: "AWS Service Catalog" is incorrect. AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS.

INCORRECT: "AWS Config" is incorrect. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resource.

INCORRECT: "AWS CodeDeploy" is incorrect. AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Lambda, and your on-premises servers.

Question 29:

A company recently setup an organization in AWS Organizations with one member account. Who pays for usage incurred by users in the AWS accounts?

- ☐ The owner of the member account pays for all usage across accounts.
- ☒ The owner of the master account pays for all usage across accounts.
(Correct)
- ☐ The owner of the master account pays for usage in the master account only.
- ☐ The owner of the member account pays for usage within their account.

Explanation

You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. Every organization in AWS Organizations has a *management account* that pays the charges of all the *member accounts*.

Consolidated billing has the following benefits:

One bill – You get one bill for multiple accounts.

Easy tracking – You can track the charges across multiple accounts and download the combined cost and usage data.

Combined usage – You can combine the usage across all accounts in the organization to share the volume pricing discounts, Reserved Instance discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts.

No extra fee – Consolidated billing is offered at no additional cost.

CORRECT: "The owner of the master account pays for all usage across accounts" is the correct answer.

INCORRECT: "The owner of the member account pays for usage within their account" is incorrect. This is not true; the member account does not pay for any usage.

INCORRECT: "The owner of the member account pays for all usage across accounts" is incorrect. This is not true; the member account does not pay for any usage.

INCORRECT: "The owner of the master account pays for usage in the master account only" is incorrect. This is not true; the master account pays for all usage across accounts.

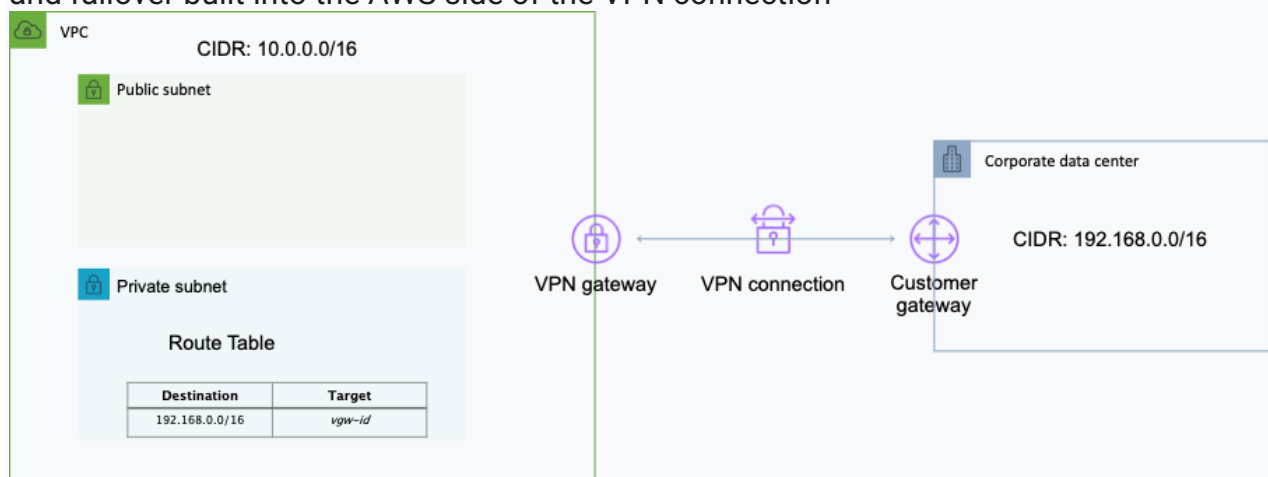
Question 30:

What can you use to quickly connect your office securely to your Amazon VPC?

- ☐ Route Table
- ☐ Direct Connect
- ☒ AWS managed VPN
(Correct)
- ☐ Internet Gateway

Explanation

An AWS managed VPN can be used to quickly connect from an office to an Amazon VPC. An Amazon VPC provides the option of creating an IPsec VPN connection between remote customer networks and their Amazon VPC over the internet, as shown in the following figure. Consider taking this approach when you want to take advantage of an AWS managed VPN endpoint that includes automated multi-data center redundancy and failover built into the AWS side of the VPN connection



CORRECT: "AWS managed VPN" is the correct answer.

INCORRECT: "Route Table" is incorrect. A Route Table is part of a VPC and is used to control how traffic is routed within the VPC.

INCORRECT: "Internet Gateway" is incorrect. An Internet Gateway is used to connect a public subnet to the Internet.

INCORRECT: "Direct Connect" is incorrect. AWS Direct Connect provides high-bandwidth, low-latency connectivity but takes weeks to months to setup (and is much more expensive).

Question 31:

Which AWS services can be used to connect the AWS Cloud and on-premises resources? (Select TWO.)

- ☒ AWS Direct Connect
(Correct)
- ☐ AWS Managed Services
- ☐ Amazon CloudHSM
- ☐ Amazon Connect
- ☒ AWS Managed VPN
(Correct)

Explanation

An AWS Managed VPN is a virtual private network connection over the public Internet. This creates an encrypted link between the on-premises network and your AWS VPC. Another way to achieve this outcome is to provision an AWS Direct Connection which connects on-premises networks to AWS using private network links.

CORRECT: "AWS Managed VPN" is a correct answer.

CORRECT: "AWS Direct Connect" is also a correct answer.

INCORRECT: "Amazon Connect" is incorrect. Amazon Connect is an easy to use omnichannel cloud contact center that helps companies provide superior customer service at a lower cost.

INCORRECT: "Amazon CloudHSM" is incorrect. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

INCORRECT: "AWS Managed Services" is incorrect. This is a managed service for lowering operational overhead and risk.

Question 32:

Which items can be configured from within the VPC management console? (Select TWO.)

- ☐ Auto Scaling
- ☒

Subnets
(Correct)

- ☐ Load Balancing
- ☒ Regions
- ☐ Security Groups
(Correct)

Explanation

Subnets and Security groups can be configured from within the VPC console.

CORRECT: "Subnets" is the correct answer.

CORRECT: "Security Groups" is the correct answer.

INCORRECT: "Regions" is incorrect. Regions are not configured, resources within regions are configured.

INCORRECT: "Load Balancing" is incorrect. Load balancing is configured from the EC2 console.

INCORRECT: "Auto Scaling" is incorrect. Auto scaling is configured from the EC2 console.

Question 33:

When storing sensitive company data in Amazon S3, which security best practices should customers follow?

- ☐ Enable AWS WAF to restrict access to the bucket.
- ☐ Enable cross-Region replication on the S3 bucket.
- ☐ Enable requester pays to reduce costs.
- ☒ Enable S3 server-side encryption on the S3 bucket.
(Correct)

Explanation

AWS recommend enabling encryption of data at rest. One of the options for encrypting data in S3 is to enable server-side encryption on the S3 bucket. With Server-side encryption, Amazon S3 encrypts objects before saving them to disks in the AWS data centers and then decrypts the objects when they are downloaded.

CORRECT: "Enable S3 server-side encryption on the S3 bucket" is the correct answer.

INCORRECT: "Enable cross-Region replication on the S3 bucket" is incorrect. This can help with adding additional redundancy for data but encrypting sensitive data is a better answer.

INCORRECT: "Enable requester pays to reduce costs" is incorrect. This is not a security best practice.

INCORRECT: "Enable AWS WAF to restrict access to the bucket" is incorrect. You cannot use AWS WAF to restrict access to an Amazon S3 bucket.

Question 34:

A company has a website that delivers static content from an Amazon S3 bucket to users from around the world. Which AWS service will deliver the content with low latency?

- ☒ Amazon CloudFront
(Correct)
- ☐ AWS Lambda
- ☐ AWS Elastic Beanstalk
- ☐ AWS Global Accelerator

Explanation

Amazon CloudFront is a content delivery network (CDN) and can use an Amazon S3 bucket configured as a static website as an origin for the content. CloudFront reduces latency for global users by serving the requested content from a local cache.

CORRECT: "Amazon CloudFront" is the correct answer.

INCORRECT: "AWS Lambda" is incorrect. Lambda is a serverless compute service that runs code in response to triggers.

INCORRECT: "AWS Elastic Beanstalk" is incorrect. Elastic Beanstalk is a platform as a service offering that is used to run applications on a managed platform.

INCORRECT: "AWS Global Accelerator" is incorrect. Global Accelerator is used to direct traffic to application endpoints in different Regions using the AWS global network. It does not cache content and would not be used in front of an S3 bucket.

Question 35:

What considerations are there when choosing which region to use? (Select TWO.)

- ☐ Available compute capacity
- ☐ Data sovereignty
(Correct)
- ☒ Latency
(Correct)
- ☒ Pricing in local currency

- ☐ Available storage capacity

Explanation

You may choose a region to reduce latency, minimize costs, or address regulatory requirements.

Latency is the delay caused mostly by distance. This means you should choose to create your buckets in Regions that are closer (physically) to your users.

Some countries or industries have regulations that mandate data must not leave a jurisdiction or country border. In this case you simply select an AWS Region accordingly.

CORRECT: "Data sovereignty" is a correct answer.

CORRECT: "Latency" is also a correct answer.

INCORRECT: "Available storage capacity" is incorrect. Available capacity is generally not a concern as AWS has a large pool of resources and does not disclose the available capacity in each region.

INCORRECT: "Pricing in local currency" is incorrect. Pricing for AWS services is in USD

INCORRECT: "Available compute capacity" is incorrect. Available capacity is generally not a concern as AWS has a large pool of resources and does not disclose the available capacity in each region.

Question 36:

Which service supports the resolution of public domain names to IP addresses or AWS resources?

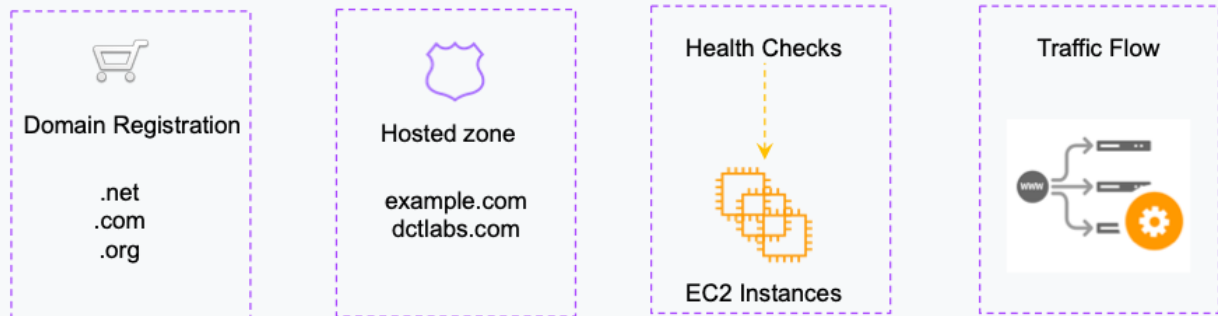
- ☐ Amazon SNS
- ☐ Amazon CloudFront
- ☐ Hosted Zones
- ☒ Amazon Route 53
(Correct)

Explanation

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) service using hosted zones. It can also be used for domain registration, health checks, and traffic flow.



Amazon Route 53



CORRECT: "Amazon Route 53" is the correct answer.

INCORRECT: "Amazon CloudFront" is incorrect. CloudFront is a content delivery network (CDN) that allows you to store (cache) your content at "edge locations" located around the world

INCORRECT: "Amazon SNS" is incorrect. Simple Notification Service is used to send notifications over multiple transport protocols.

INCORRECT: "Hosted Zones" is incorrect. A hosted zone is a collection of records for a specified domain in Route 53.

Question 37:

Which benefits can an organization achieve by deploying AWS Global Accelerator?
(Select TWO.)

- ☒ Decreased latency to reach applications deployed on AWS.
(Correct)
- ☒ It caches content around the world to reduce latency.
- ☐ Reduces the cost of deploying global services on AWS.
- ☐ It increases the durability of data stored on Amazon S3.
- ☐ Improves the availability of applications on AWS.
(Correct)

Explanation

AWS Global Accelerator is a service that improves the availability and performance of applications with local or global users.

It provides static IP addresses that act as a fixed entry point to application endpoints in a single or multiple AWS Regions, such as Application Load Balancers, Network Load Balancers or EC2 instances.

Uses the AWS global network to optimize the path from users to applications, improving the performance of TCP and UDP traffic.

CORRECT: "Improves the availability of applications on AWS" is a correct answer.

CORRECT: "Decreased latency to reach applications deployed on AWS" is also a correct answer.

INCORRECT: "Reduces the cost of deploying global services on AWS" is incorrect. Global Accelerator is not used for cost reduction.

INCORRECT: "It increases the durability of data stored on Amazon S3" is incorrect. Global Accelerator is not related to Amazon S3.

INCORRECT: "It caches content around the world to reduce latency" is incorrect. Do not confuse AWS Global Accelerator with Amazon CloudFront which does cache content.

Question 38: **Correct**

A customer needs to determine Total Cost of Ownership (TCO) for a workload that requires physical isolation. Which hosting model should be accounted for?

- ☒ Dedicated Hosts
(Correct)
- ☐ On-Demand Instances
- ☐ Reserved Instances
- ☐ Spot Instances

Explanation

An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts allow you to use your existing per-socket, per-core, or per-VM software licenses, including Windows Server, Microsoft SQL Server, SUSE, and Linux Enterprise Server.

Note that dedicated hosts can be considered "hosting model" as it determines that actual underlying infrastructure that is used for running your workload. All of the other answers are simply pricing plans for shared hosting models.

CORRECT: "Dedicated Hosts" is the correct answer.

INCORRECT: "Reserved Instances" is incorrect as this pricing model does not support physical isolation.

INCORRECT: "On-Demand Instances" is incorrect as this pricing model does not support physical isolation.

INCORRECT: "Spot Instances" is incorrect as this hosting pricing does not support physical isolation.

Question 39:

Which Amazon S3 storage classes should be used for storing data for long time periods when immediate access is not required at the LOWEST cost? (Select TWO.)

- ☐ Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)
- ☐ Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
- ☒ Amazon S3 Glacier
(Correct)
- ☒ Amazon S3 Glacier Deep Archive
(Correct)
- ☐ Amazon S3 Standard

Explanation

Amazon S3 Glacier and Amazon S3 Glacier Deep Archive are suitable for archiving data for long time periods and both classes offer extremely low costs. With both of these storage classes you cannot access data immediately.

	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

CORRECT: "Amazon S3 Glacier" is a correct answer.

CORRECT: "Amazon S3 Glacier Deep Archive" is also a correct answer.

INCORRECT: "Amazon S3 Standard-Infrequent Access (S3 Standard-IA)" is incorrect. This storage class is suited to data that requires immediate access infrequently.

INCORRECT: "Amazon S3 Standard" is incorrect as this is a more expensive storage class suitable for general needs.

INCORRECT: "Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect. This storage class is suited to data that requires lower resiliency.

Question 40:

What is the scope of a VPC within a region?

- ☐ At least 2 subnets per region
- ☐ At least 2 data centers per region
- ☒ Spans all Availability Zones within the region
(Correct)
- ☐ Spans all Availability Zones globally

Explanation

An Amazon Virtual Private Cloud (VPC) spans all availability zones within a region.

CORRECT: "Spans all Availability Zones within the region" is the correct answer.

INCORRECT: "Spans all Availability Zones globally" is incorrect. VPCs do not span regions, you create VPCs in each region.

INCORRECT: "At least 2 subnets per region" is incorrect. VPCs are not limited by subnets, subnets are created within AZs and you can have many subnets in an AZ

INCORRECT: "At least 2 data centers per region" is incorrect. An AZ uses one or more data centers. AWS does not publicize the details.

Question 41:

A company has been using an AWS managed IAM policy for granting permissions to users but needs to add some permissions.

How can this be achieved?

- ☐ Create a rule in AWS WAF.
- ☐ Create a Service Control Policy.
- ☒ Edit the AWS managed policy.
- ☐ Create a custom IAM policy.
(Correct)

Explanation

AWS managed policies cannot be edited so if you need to add permissions to users that are not granted in the policy you must create your own custom IAM policy.

CORRECT: "Create a custom IAM policy" is the correct answer.

INCORRECT: "Edit the AWS managed policy" is incorrect. You cannot edit AWS managed policies.

INCORRECT: "Create a Service Control Policy" is incorrect. SCPs are used in AWS Organizations to restrict available permissions. They do not grant permissions.

INCORRECT: "Create a rule in AWS WAF" is incorrect. WAF is a web application firewall used for protecting resources from web-based attacks.

Question 42:

A company needs to optimize costs and resource usage through monitoring of operational health for all resources running on AWS.

Which AWS service will meet these requirements?

- ☒ AWS CloudTrail
- ☐ AWS Control Tower
- ☐ Amazon CloudWatch
(Correct)
- ☐ AWS Config

Explanation

Amazon CloudWatch is a performance monitoring tool that receives metrics from AWS services. This data can be used for monitoring the operational health of resources as well as being used to optimize costs through ensuring systems are right-sized and just enough capacity is provisioned.

CORRECT: "Amazon CloudWatch" is the correct answer.

INCORRECT: "AWS Control Tower" is incorrect. AWS Control Tower is a service that is intended for organizations with multiple accounts and teams who are looking for the easiest way to set up their new multi-account AWS environment and govern at scale

INCORRECT: "AWS CloudTrail" is incorrect. CloudTrail is used for auditing (who did what and when), it is not used for monitoring operational health.

INCORRECT: "AWS Config" is incorrect. Config is used for managing compliance for AWS services.

Question 43:

Under the AWS shared responsibility model what is the customer responsible for? (Select TWO.)

- ☒ Encryption of customer data
(Correct)

- ☐ Replacement and disposal of disk drives
- ☐ Patch management of infrastructure
- ☒ Configuration of security groups
(Correct)
- ☐ Physical security of the data center

Explanation

AWS are responsible for “Security **of** the Cloud” and customers are responsible for “Security **in** the Cloud”.

AWS are responsible for items such as the physical security of the DC, replacement of old disk drives, and patch management of the infrastructure

Customers are responsible for items such as configuring security groups, network ACLs, patching their operating systems and encrypting their data

CORRECT: "Configuration of security groups" is a correct answer.

CORRECT: "Encryption of customer data" is also a correct answer.

INCORRECT: "Physical security of the data center" is incorrect as this is an AWS responsibility.

INCORRECT: "Replacement and disposal of disk drives" is incorrect as this is an AWS responsibility.

INCORRECT: "Patch management of infrastructure" is incorrect as this is an AWS responsibility.

Question 44:

Under the shared responsibility model, what are examples of shared controls? (Select TWO.)

- ☐ Service and Communications Protection
- ☒ Patch management
(Correct)
- ☐ Storage system patching
- ☒ Configuration management
(Correct)
- ☐ Physical and environmental

Explanation

Shared Controls– Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives

Patch Management– AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications

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

CORRECT: "Patch management" is a correct answer.

CORRECT: "Configuration management" is also a correct answer.

INCORRECT: "Storage system patching" is incorrect. Storage system patching is an AWS responsibility.

INCORRECT: "Physical and environmental" is incorrect. Physical and Environmental controls is an example of an inherited control (a customer fully inherits from AWS).

INCORRECT: "Service and Communications Protection" is incorrect. Service and Communications Protection is an example of a customer specific control.

Question 45:

Which feature of Amazon Rekognition can assist with saving time?

- ☐ Identification of the language of text in a document
- ☐ Provides on-demand access to compliance-related information
- ☒ Identification of objects in images and videos
(Correct)
- ☐ Adds automatic speech recognitions (ASR) to applications

Explanation

Amazon Rekognition makes it easy to add image and video analysis to your applications. You just provide an image or video to the Rekognition API, and the service can identify the objects, people, text, scenes, and activities, as well as detect any inappropriate content.

CORRECT: "Identification of objects in images and videos" is the correct answer.

INCORRECT: "Identification of the language of text in a document" is incorrect. Amazon Comprehend identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; analyzes text using tokenization and parts of speech; and automatically organizes a collection of text files by topic.

INCORRECT: "Adds automatic speech recognitions (ASR) to applications" is incorrect. Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for developers to add speech-to-text capability to their applications

INCORRECT: "Provides on-demand access to compliance-related information" is incorrect. AWS Artifact is a resource for compliance-related information. It provides on-demand access to AWS' security and compliance reports and select online agreements

Question 46:

A large company is interested in avoiding long-term contracts and moving from fixed costs to variable costs.

What is the value proposition of AWS for this company?

- ☐ Volume pricing discounts
- ☐ Automated cost optimization
- ☒ Pay-as-you-go pricing
(Correct)
- ☐ Economies of scale

Explanation

Pay-as-you-go pricing helps companies move away from fixed costs to variable costs in a model in which they only pay for what they actually use. There are no fixed term contracts with AWS so that requirement is also met.

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

INCORRECT: "Economies of scale" is incorrect. You do get good pricing because of the economies of scale leveraged by AWS. However, the value proposition for companies wishing to avoid fixed costs is pay-as-you-go pricing. This flexibility can be more important in some cases than the actual cost per unit.

INCORRECT: "Volume pricing discounts" is incorrect. This is not the value proposition for this company as they are seeking to avoid long-term contracts and fixed costs, not to achieve a discount.

INCORRECT: "Automated cost optimization" is incorrect. This is a not a feature that relates to the value proposition for this customer.

Question 47:

What advantages does deploying Amazon CloudFront provide? (Select TWO.)

- ☐ Provides serverless compute services
- ☒ Improved performance for end users
(Correct)

- ☐ Automated deployment of resources
- ☐ A private network link to the AWS cloud
- ☒ Reduced latency
(Correct)

Explanation

content at “edge locations” located around the world. This allows customers to access content more quickly and provides security against DDoS attacks. CloudFront can be used for data, videos, applications, and APIs.

CORRECT: "Reduced latency" is a correct answer.

CORRECT: "Improved performance for end users" is also a correct answer.

INCORRECT: "A private network link to the AWS cloud" is incorrect. A private network link to the AWS cloud can be provisioned using AWS Direct Connect or an IPSec VPN

INCORRECT: "Automated deployment of resources" is incorrect. Automated deployment of resources is performed using CloudFormation.

INCORRECT: "Provides serverless compute services" is incorrect. CloudFront is a CDN not a serverless compute service

Question 48:

When a customer deploys a database on Amazon RDS, what is the customer responsible for?

- ☐ Managing automatic backups of the database
- ☒ Configuring Auto Scaling for high availability of instances
- ☐ Patching the underlying operating system
- ☐ Controlling network access through security groups
(Correct)

Explanation

The Amazon Relational Database Service (RDS) is a managed service where AWS manage administration tasks including hardware provisioning, database setup, patching and backups. The customer is responsible for configuring security groups to control access to the database.

CORRECT: "Controlling network access through security groups" is the correct answer.

INCORRECT: "Patching the underlying operating system" is incorrect as this is taken care of by AWS.

INCORRECT: "Managing automatic backups of the database" is incorrect as this is taken care of by AWS.

INCORRECT: "Configuring Auto Scaling for high availability of instances" is incorrect as you cannot use Auto Scaling with RDS for availability of the database instances.

Question 49:

Which AWS support plan should you use if you need a response time of < 15 minutes for a business-critical system failure?

- ☐ Basic
- ☐ Business
- ☒ Enterprise
(Correct)
- ☐ Developer

Explanation

Only the Enterprise plan provides a response time of < 15 minutes for the failure of a business-critical system.

Both Business and Enterprise offer < 1 hour response time for the failure of a production system.

CORRECT: "Enterprise" is the correct answer.

INCORRECT: "Business" is incorrect as described above.

INCORRECT: "Basic" is incorrect as described above.

INCORRECT: "Developer" is incorrect as described above.

Question 50:

Under the AWS shared responsibility model, what are the customer's responsibilities? (Select TWO.)

- ☐ Physical network devices including firewalls
- ☒ Data integrity authentication
(Correct)
- ☒ Security of data in transit
(Correct)
- ☐ Storage device decommissioning
- ☐ Physical and environmental security

Explanation

Under the AWS shared responsibility model, AWS are responsible for security “of” the cloud and customers are responsible for security “in” the cloud. Securing data in transit and ensuring the integrity of data are customer responsibilities. Customers are always responsible for managing data including encryption.

CORRECT: "Security of data in transit" is a correct answer.

CORRECT: "Data integrity authentication" is also a correct answer.

INCORRECT: "Physical and environmental security" is incorrect as this is security “of” the cloud and therefore the responsibility of AWS.

INCORRECT: "Physical network devices including firewalls" is incorrect as this is security “of” the cloud and therefore the responsibility of AWS.

INCORRECT: "Storage device decommissioning" is incorrect as this is security “of” the cloud and therefore the responsibility of AWS.

Question 51:

Which design principles are enabled by the AWS Cloud to improve the operation of workloads? (Select TWO.)

- ☒ Remove single points of failure
(Correct)
- ☐ Minimize platform design
- ☐ Minimum viable product
- ☒ Loose coupling
(Correct)
- ☐ Customized hardware

Explanation

Loose coupling is when you break systems down into smaller components that are loosely coupled together. This reduces interdependencies between systems components. This is achieved in the cloud using messages buses, notification and messaging services.

Removing single points of failure ensures fault tolerance and high availability. This is easily achieved in the cloud as the architecture and features of the cloud support the implementation of highly available and fault tolerant systems.

CORRECT: "Loose coupling" is a correct answer.

CORRECT: "Remove single points of failure" is also a correct answer.

INCORRECT: "Customized hardware" is incorrect. You cannot customize hardware in the cloud.

INCORRECT: "Minimize platform design" is incorrect. This is not an operational advantage for workloads in the cloud.

INCORRECT: "Minimum viable product" is incorrect. This is not an operational advantage for workloads in the cloud.

Question 52:

Which AWS service can be used to generate encryption keys that can be used to encrypt data? (Select TWO.)

- ☐ AWS Secrets Manager
- ☐ Amazon Macie
- ☐ AWS Certificate Manager
- ☒ AWS CloudHSM
(Correct)
- ☒ AWS Key Management Service (AWS KMS)
(Correct)

Explanation

Both AWS KMS and AWS CloudHSM can be used to generate data encryption keys. You use what are called customer master keys (CMKs) to create data encryption keys. The data encryption keys can then be used to actually encrypt the data.

CORRECT: "AWS Key Management Service (AWS KMS)" is a correct answer.

CORRECT: "AWS CloudHSM" is also a correct answer.

INCORRECT: "Amazon Macie" is incorrect. Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS

INCORRECT: "AWS Certificate Manager" is incorrect. AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

INCORRECT: "AWS Secrets Manager" is incorrect. 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.

Question 53:

Which benefit of the AWS Cloud eliminates the need for users to try estimating future infrastructure usage?

- ☒ Elasticity of the AWS Cloud
(Correct)

- ☐ Economies of scale
- ☐ Security of the AWS Cloud
- ☐ Easy global deployments

Explanation

Elasticity means that your infrastructure scales based on actual usage. When you have higher demand you use more infrastructure and pay more and when you have less demand you need less infrastructure and pay less. The benefits are you don't need to guess about capacity and pay only for what you actually need.

CORRECT: "Elasticity of the AWS Cloud" is the correct answer.

INCORRECT: "Easy global deployments" is incorrect. It is easy to deploy many AWS resources globally but this benefit does not eliminate the need to estimate future usage.

INCORRECT: "Security of the AWS Cloud" is incorrect. The security of the AWS Cloud is important but does not eliminate the need to estimate future usage.

INCORRECT: "Economies of scale" is incorrect. This means you pay less for some resources because of the benefits of AWS's scale. However, this benefit does not eliminate the need to estimate future usage.

Question 54:

What strategy can assist with allocating metadata to AWS resources for cost tracking and visibility?

- ☐ Access Control
- ☐ Categorizing
- ☒ Tagging
(Correct)
- ☐ Labelling

Explanation

AWS allows customers to assign metadata to their AWS resources in the form of *tags*. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. AWS Cost Explorer and detailed billing reports support the ability to break down AWS costs by tag.

The other options are incorrect as they are not methods of adding metadata to an AWS resource.

CORRECT: "Tagging" is the correct answer.

INCORRECT: "Labelling" is incorrect as explained above.

INCORRECT: "Access Control" is incorrect as explained above.

INCORRECT: "Categorizing" is incorrect as explained above.

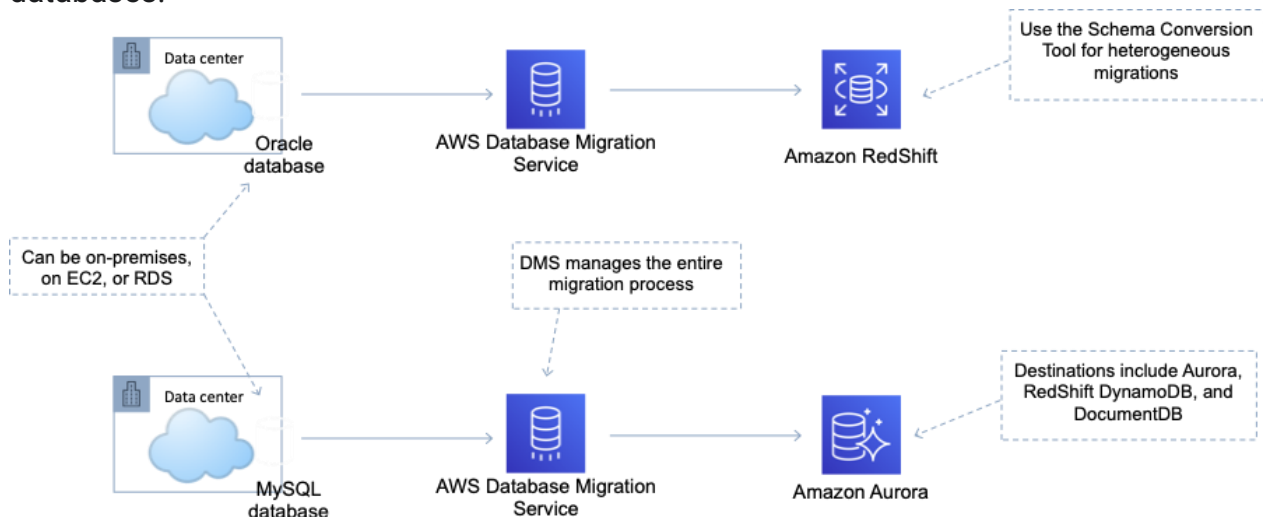
Question 55:

Which service can be used to help you to migrate databases to AWS quickly and securely?

- ☐ AWS Key Management Service (KMS)
- ☒ AWS Database Migration Service (DMS)
(Correct)
- ☐ AWS DataSync
- ☐ AWS Server Migration Service (SMS)

Explanation

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



CORRECT: "AWS Database Migration Service (DMS)" is the correct answer.

INCORRECT: "AWS Server Management Service (SMS)" is incorrect. AWS Server Migration Service (SMS) is used to migrate virtual machines not databases.

INCORRECT: "AWS Key Management Service (KMS)" is incorrect. AWS Key Management Service (KMS) is used for managing encryption keys.

INCORRECT: "AWS DataSync" is incorrect. This service is used for migrating data from network attached storage (NAS) devices to AWS. It is not used for databases.

Question 56:

A company stores copies of backups on Amazon S3 and requires rapid access but low resiliency. Which storage class is optimized for these requirements?

- ☐

Amazon S3 Standard

- ☒ Amazon S3 One Zone-Infrequent Access
(Correct)
- ☐ Amazon S3 Glacier
- ☐ Amazon S3 Glacier Deep Archive

Explanation

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 and costs 20% less than S3 Standard-IA.

S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA.

It's a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.

CORRECT: "Amazon S3 One Zone-Infrequent Access" is the correct answer.

INCORRECT: "Amazon S3 Standard" is incorrect as this is a more resilient storage class and will cost more so it not optimized for these requirements.

INCORRECT: "Amazon S3 Glacier Deep Archive" is incorrect. This storage class is suited to archival and takes several hours to restore data.

INCORRECT: "Amazon S3 Glacier" is incorrect. This storage class is suited to archival and takes minutes to hours to restore data.

Question 57:

Which service allows you to automatically expand and shrink your application in response to demand?

- ☐ AWS ElastiCache
- ☐ Amazon DynamoDB
- ☒ Amazon EC2 Auto Scaling
(Correct)
- ☐ Amazon Elastic Load Balancing

Explanation

Amazon EC2 Auto Scaling automatically responds to demand by adding or removing EC2 instances to ensure the right amount of compute capacity is available at any time. This can help to automatically adjust the number of instances based on the load on your application.

CORRECT: "Amazon EC2 Auto Scaling" is the correct answer.

INCORRECT: "AWS ElastiCache" is incorrect. AWS ElastiCache provides in-memory cache and database services

INCORRECT: "Amazon Elastic Load Balancing" is incorrect. Amazon ELB distributes incoming requests to EC2 instances. It can be used in conjunction with Auto Scaling

INCORRECT: "Amazon DynamoDB" is incorrect. DynamoDB is a non-relational (NoSQL)

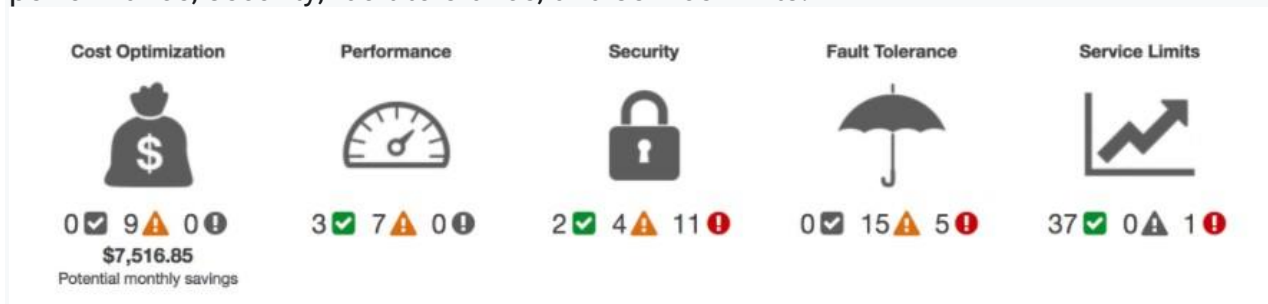
Question 58:

AWS Trusted Advisor provides real-time guidance on what characteristics of an AWS account? (Select TWO.)

- ☐ Application performance
- ☒ Security best practices
(Correct)
- ☐ Application configuration
- ☐ Network utilization
- ☒ Cost optimization
(Correct)

Explanation

AWS Trusted Advisor provides real-time guidance to help customers provision resources following AWS best practices. The service offers guidance for cost optimization, performance, security, fault tolerance, and service limits.



CORRECT: "Security best practices" is a correct answer.

CORRECT: "Cost optimization" is also a correct answer.

INCORRECT: "Application performance" is incorrect as Trusted Advisor offers advice on AWS resources, not on applications.

INCORRECT: "Network utilization" is incorrect. CloudWatch should be used for gaining insights into metrics relating to network utilization.

INCORRECT: "Application configuration" is incorrect as Trusted Advisor offers advice on AWS resources, not on applications.

Question 59:

Which of the following AWS services are compute services? (Select TWO.)

- ☐ Amazon EFS
- ☒ 1. AWS Elastic Beanstalk
(Correct)
- ☒ AWS Batch
(Correct)
- ☐ Amazon Inspector
- ☐ AWS CloudTrail

Explanation

AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

CORRECT: "AWS Batch" is a correct answer.

CORRECT: "AWS Elastic Beanstalk" is also a correct answer.

INCORRECT: "AWS CloudTrail" is incorrect. CloudTrail is used for auditing.

INCORRECT: "Amazon EFS" is incorrect. The Elastic File System (EFS) is used for storing data and is mounted by EC2 instances.

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

Question 60:

Which feature can you use to grant read/write access to an Amazon S3 bucket?

- ☐ IAM User
- ☒ IAM Policy
(Correct)
- ☐ IAM Role
- ☐ IAM Group

Explanation

Identity and access management (IAM) Policies are documents that define permissions and can be applied to users, groups and roles. IAM policies can be written to grant access to Amazon S3 buckets.

CORRECT: "IAM Policy" is the correct answer.

INCORRECT: "IAM Role" is incorrect. IAM Roles are created and then "assumed" by trusted entities and define a set of permissions for making AWS service requests.

INCORRECT: "IAM Group" is incorrect. IAM Groups are collections of users and have policies attached to them.

INCORRECT: "IAM User" is incorrect. An IAM user is an entity that represents a person or service.

Question 61:

A user is planning to launch three EC2 instances behind a single Elastic Load Balancer. The deployment should be highly available.

- ☒ Launch the instances as EC2 Reserved Instances in the same AWS Region, but in different Availability Zones.
- ☐ Launch the instances as EC2 Spot Instances in the same AWS Region and the same Availability Zone.
- ☐ Launch the instances in multiple AWS Regions, and use Elastic IP addresses.
- ☐ Launch the instances across multiple Availability Zones in a single AWS Region. (Correct)

Explanation

To make the deployment highly available the user should launch the instances across multiple Availability Zones in a single AWS Region. Elastic Load Balancers can only serve targets in a single Region so it is not possible to deploy across Regions.

CORRECT: "Launch the instances across multiple Availability Zones in a single AWS Region" is the correct answer.

INCORRECT: "Launch the instances as EC2 Spot Instances in the same AWS Region and the same Availability Zone" is incorrect. The pricing model is not relevant to high availability and deploying in a single AZ does not result in a highly available deployment.

INCORRECT: "Launch the instances in multiple AWS Regions, and use Elastic IP addresses" is incorrect. You cannot use an ELB with instances in multiple Regions and using an EIP does not help.

INCORRECT: "Launch the instances as EC2 Reserved Instances in the same AWS Region, but in different Availability Zones" is incorrect. Using reserved instances may not be appropriate as we do not know whether this is going to be a long-term workload or not.

Question 62:

Which AWS service or feature can be used to restrict the individual API actions that users and roles in each member account can access?

- ☐ Amazon Macie
- ☒ AWS Organizations
(Correct)
- ☐ AWS Shield
- ☐ AWS IAM

Explanation

AWS Organizations offers Service control policies (SCPs) which are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions (API actions) for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled.

CORRECT: "AWS Organizations" is the correct answer.

INCORRECT: "Amazon Macie" is incorrect. Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS

INCORRECT: "AWS Shield" is incorrect. AWS Shield a service that protects workloads against distributed denial of service (DDoS) attacks.

INCORRECT: "AWS IAM" is incorrect. AWS IAM is used for assigning permissions but SCPs in AWS Organizations are used to control which API actions are allowed in an account. You need to be granted permission in IAM and have the API allowed to be able to use the API successfully.

Question 63:

Which of the following types of recommendation does AWS Trusted Advisor provide? (Select TWO.)

- ☐ Performance
(Correct)
- ☒ Serverless architecture
- ☐ Replatforming
- ☒ Cost optimization
(Correct)

- ☐ Access auditing

Explanation

AWS Trusted Advisor provides real-time guidance to help customers provision resources following AWS best practices. The service offers guidance for cost optimization, performance, security, fault tolerance, and service limits.



CORRECT: "Cost optimization" is a correct answer.

CORRECT: "Performance" is also a correct answer.

INCORRECT: "Access auditing" is incorrect. You should use AWS CloudTrail for auditing.

INCORRECT: "Serverless architecture" is incorrect. Trusted Advisor does not offer advice on using serverless architectures.

INCORRECT: "Replatforming" is incorrect. Trusted Advisor does not offer advice on replatforming applications.

Question 64:

A Cloud Practitioner needs to decide which Amazon S3 storage class to use for storing copies of backup data. The storage must provide rapid access when needed but resiliency can be low. Which storage class is most suitable?

- ☐ Amazon S3 Glacier Deep Archive
- ☒ Amazon S3 One Zone-IA
(Correct)
- ☐ Amazon S3 Glacier
- ☐ Amazon S3 Standard

Explanation

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 and costs 20% less than S3 Standard-IA.

	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

CORRECT: "Amazon S3 One Zone-IA" is the correct answer.

INCORRECT: "Amazon S3 Standard" is incorrect. This storage class provides higher durability and availability but costs more.

INCORRECT: "Amazon S3 Glacier Deep Archive" is incorrect. This storage class is used for archiving so data cannot be immediately accessed.

INCORRECT: "Amazon S3 Glacier" is incorrect. This storage class is used for archiving so data cannot be immediately accessed.

Question 65:

Which AWS service or component allows inbound traffic from the internet to access a VPC?

- ☐ Virtual Private Gateway
- ☐ NAT Gateway
- ☐ VPC Route Table
- ☒ Internet gateway
(Correct)

Explanation

An Internet gateway is attached to a VPC and allows inbound traffic from the internet to access the VPC. It is also used as a target in route tables for outbound internet traffic.

CORRECT: "Internet gateway" is the correct answer.

INCORRECT: "NAT Gateway" is incorrect. A NAT gateway is used for outbound internet access for instances running in a private subnet.

INCORRECT: "VPC Route Table" is incorrect. The route table is used within a VPC for directing traffic.

INCORRECT: "Virtual Private Gateway" is incorrect. A VGW is used for IPSec VPN connections to access a VPC.