AWS Cloud Practitioner - Practice Test 3

**1. Question**

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
  + **WAF can check for the presence of SQL code that is likely to be malicious (known as SQL injection)**
  + AWS WAF lets you monitor the HTTP and HTTPS requests that are forwarded to Amazon Route 53
  + **WAF can block all requests except the ones that you specify**
  + WAF offers protection against all known infrastructure (Layer 3 and 4) attacks

**Unattempted**

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 24×7 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>

**2. Question**

Which of the following AWS services offer LifeCycle Management for cost-optimal storage?

* + Amazon EBS
  + **Amazon S3**
  + AWS Storage Gateway
  + Amazon Instance Store

**Unattempted**

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>

**3. Question**

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?

* + CloudFormation
  + **Systems Manager**
  + OpsWorks
  + Config

**Unattempted**

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/>

**4. Question**

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**
  + Go global in minutes
  + Trade capital expense for variable expense
  + Increased speed and agility

**Unattempted**

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>

**5. Question**

Which of the following is a container service of AWS?

* + AWS Elastic Beanstalk
  + Amazon Simple Notification Service
  + Amazon SageMaker
  + **AWS Fargate**

**Unattempted**

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/>

**6. Question**

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

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

**Unattempted**

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.  
 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>

**7. Question**

AWS Marketplace facilitates which of the following use-cases? (Select two)

* + Purchase compliance documents from third-party vendors
  + **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**
  + Raise request for purchasing AWS Direct Connect connection
  + Buy Amazon EC2 Standard Reserved Instances

**Unattempted**

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>

**8. Question**

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

* + S3 Glacier
  + S3 One Zone-IA
  + **S3 Standard**
  + S3 Standard-IA
  + **S3 Intelligent-Tiering**

**Unattempted**

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:  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/>

**9. Question**

Which of the following S3 storage classes has NO constraint of a minimum storage duration charge for objects?

* + S3 One Zone-IA
  + **S3 Standard**
  + S3 Glacier
  + S3 Intelligent-Tiering

**Unattempted**

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:  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/>

**10. Question**

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?

* + AWS Direct Connect
  + Site to Site VPN
  + VPC Endpoint
  + **VPC Peering**

**Unattempted**

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>

**11. Question**

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

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

**Unattempted**

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:  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>

**12. Question**

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

* + **Amazon Relational Database Service (Amazon RDS)**
  + Amazon Simple Storage Service (Amazon S3)
  + AWS Identity & Access Management (IAM)
  + Amazon CloudFront
  + **Amazon Elastic Compute Cloud (Amazon EC2)**

**Unattempted**

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>

**13. Question**

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 Shield Standard**
  + AWS Web Application Firewall (WAF)
  + Security Groups for Amazon EC2

**Unattempted**

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 24×7 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/>

**14. Question**

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

* + Amazon Route 53
  + S3 Transfer Acceleration
  + AWS Global Accelerator
  + **Amazon CloudFront**

**Unattempted**

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 [http://www.example.com](http://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/>

**15. Question**

Which of the following statements are true regarding Amazon Simple Storage Service (S3) (Select two)?

* + **S3 is a key value based object storage service**
  + S3 is a fully managed, elastic file system storage service used as database backup
  + You can install databases on S3
  + S3 is a block storage service designed for a broad range of workloads
  + **S3 stores data in a flat non-hierarchical structure**

**Unattempted**

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/>

**16. Question**

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**
  + Hardware MFA device

**Unattempted**

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:  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>

**17. Question**

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

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

**Unattempted**

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/>

**18. Question**

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?

* + AWS Global Accelerator
  + AWS Direct Connect
  + Amazon CloudFront
  + **S3 Transfer Acceleration**

**Unattempted**

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/>

**19. Question**

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

* + **IAM role**
  + AWS IAM user access keys
  + AWS Key Management Service
  + Amazon Cognito

**Unattempted**

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>

**20. Question**

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 Bucket Policy
  + **Amazon S3 Replication**
  + Amazon S3 Transfer Acceleration

**Unattempted**

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:  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>

**21. Question**

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

* + **Amazon ElastiCache**
  + Amazon Athena
  + Amazon DynamoDB
  + Amazon RDS

**Unattempted**

Correct option:  
Amazon ElastiCache  
Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-Source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for real-time use cases like Caching, Session Stores, Gaming, Geospatial Services, Real-Time Analytics, and Queuing. ElastiCache cannot be used for online analytical processing.  
How ElastiCache Works:  via – https://aws.amazon.com/elasticache/  
Incorrect options:  
Amazon RDS – Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. RDS cannot be used as an in-memory database.  
Amazon DynamoDB – Amazon DynamoDB is a NoSQL database that supports key-value and document data models and enables developers to build modern, serverless applications that can start small and scale globally to support petabytes of data and tens of millions of read and write requests per second. DynamoDB supports both key-value and document data models. This enables DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases. DynamoDB cannot be used as an in-memory database.  
Amazon Athena – Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. Athena cannot be used as an in-memory database.  
Reference:  
<https://aws.amazon.com/elasticache/>

**22. Question**

Which AWS service can be used to automate code deployment to EC2 instances as well as on-premises instances?

* + **AWS CodeDeploy**
  + AWS CloudFormation
  + AWS CodePipeline
  + AWS CodeCommit

**Unattempted**

Correct option:  
AWS CodeDeploy  
AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone manual operations, and the service scales with your infrastructure so you can easily deploy to one instance or thousands.  
Incorrect options:  
AWS CodeCommit – AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. It cannot be used to automate code deployment.  
AWS CloudFormation – AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. It cannot be used to automate code deployment.  
AWS CodePipeline – AWS CodePipeline is a continuous delivery service that enables you to model, visualize, and automate the steps required to release your software. With AWS CodePipeline, you model the full release process for building your code, deploying to pre-production environments, testing your application and releasing it to production.  
AWS CodePipeline integrates with AWS services such as AWS CodeCommit, Amazon S3, AWS CodeBuild, AWS CodeDeploy, AWS Elastic Beanstalk, AWS CloudFormation, AWS OpsWorks, Amazon ECS, and AWS Lambda. To further elucidate, CodePipeline cannot by itself deploy the code, it can integrate with CodeDeploy for the actual deployment.  
How CodePipeline Works:  via – https://aws.amazon.com/codepipeline/  
Reference:  
<https://aws.amazon.com/codedeploy/>

**23. Question**

Which pillar of the AWS Well-Architected Framework recommends maintaining infrastructure as code?

* + **Operational Excellence**
  + Security
  + Cost Optimization
  + Performance Efficiency

**Unattempted**

Correct option:  
Operational Excellence  
The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement.  
The AWS Well-Architected Framework is based on five pillars — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.  
The Operational Excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events.  
Incorrect options:  
Cost Optimization – Cost Optimization focuses on avoiding un-needed costs. Key topics include understanding and controlling where the money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.  
Performance Efficiency – The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.  
Security – The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.  
Reference:  
<https://wa.aws.amazon.com/wat.pillar.operationalExcellence.en.html>

**24. Question**

Which AWS services support High Availability by default? (Select two)

* + EBS
  + Redshift
  + **EFS**
  + Instance Store
  + **DynamoDB**

**Unattempted**

Correct options:  
DynamoDB – Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It’s a fully managed, multi-Region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in high availability and data durability.  
DynamoDB High Availability:  via – https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html  
EFS – Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability.  
EFS High Availability:  via – https://aws.amazon.com/efs/faq/  
Incorrect options:  
Redshift – Amazon Redshift is a fast, fully managed cloud data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools.  
Amazon Redshift only supports Single-AZ deployments:  via – https://aws.amazon.com/redshift/faqs/  
EBS – Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. EBS volumes are replicated within an Availability Zone (AZ) and can easily scale to petabytes of data.  
Instance Store – As Instance Store volumes are tied to an EC2 instance, they are also single AZ entities.  
References:  
<https://aws.amazon.com/efs/faq/>  
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>  
<https://aws.amazon.com/redshift/faqs/>  
<https://aws.amazon.com/ebs/>

**25. Question**

Which of the following is a part of the AWS Global Infrastructure?

* + **Region**
  + Virtual Private Network (VPN)
  + Subnets
  + Virtual Private Cloud (VPC)

**Unattempted**

Correct option:  
Region  
AWS Region is a physical location around the world where AWS builds its data centers. Each group of logical data centers is called an Availability Zone (AZ). Each AWS Region consists of multiple, isolated, and physically separate AZ’s within a geographic area.  
Please see this illustration for AWS regions in the US:  via – https://aws.amazon.com/about-aws/global-infrastructure/regions\_az/  
Incorrect options:  
Virtual Private Cloud (VPC) – Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including the selection of your IP address range, creation of subnets, and configuration of route tables and network gateways. A VPC spans all of the Availability Zones in the Region.  
Virtual Private Network (VPN) – AWS Virtual Private Network (AWS VPN) lets you establish a secure and private encrypted tunnel from your on-premises network to the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN.  
Subnets – A subnet is a range of IP addresses within your VPC. A subnet spans only one Availability Zone in the Region.  
These three options are not a part of the AWS Global Infrastructure.  
Reference:  
<https://aws.amazon.com/about-aws/global-infrastructure/regions_az/>

**26. Question**

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

* + **Virtual MFA device**
  + U2F security key
  + Soft Token MFA device
  + Hardware MFA device

**Unattempted**

Correct option:  
Virtual MFA device  
A software app that runs on a phone or other device and emulates a physical device. The device generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each virtual MFA device assigned to a user must be unique. A user cannot type a code from another user’s virtual MFA device to authenticate.  
Google Authenticator is an example of a Virtual MFA device:   
Incorrect options:  
U2F security key – A device that you plug into a USB port on your computer. U2F is an open authentication standard hosted by the FIDO Alliance. When you enable a U2F security key, you sign in by entering your credentials and then tapping the device instead of manually entering a code.  
Hardware MFA device – A hardware device that generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each MFA device assigned to a user must be unique. A user cannot type a code from another user’s device to be authenticated.  
Soft Token MFA device – This is a made-up option and has been added as a distractor.  
Reference:  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html>

**27. Question**

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

* + Convert images into greyscale
  + Resize images quickly
  + **Identify objects in a photo**
  + Human pose detection

**Unattempted**

Correct option:  
Identify objects in a photo  
With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.  
Amazon Rekognition Use-Cases:  
 via – https://aws.amazon.com/rekognition/  
 via – https://aws.amazon.com/rekognition/  
Incorrect options:  
Convert images into greyscale  
Resize images quickly  
Human pose detection  
Amazon Rekognition does not do image processing tasks such as converting images to greyscale or resizing images. Human pose detection is not available in Amazon Rekognition.  
Reference:

**28. Question**

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

* + AWS Total Cost of Ownership (TCO) Calculator
  + AWS Budgets
  + AWS Cost Explorer
  + **AWS Cost and Usage Reports**

**Unattempted**

Correct option:  
AWS Cost and Usage Reports  
The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself. AWS updates the report in your bucket once a day in comma-separated value (CSV) format.  
AWS Cost and Usage Reports Overview:  via – https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html  
Incorrect options:  
AWS Total Cost of Ownership (TCO) Calculator – TCO calculator helps to compare the cost of your applications in an on-premises or traditional hosting environment to AWS. AWS helps reduce Total Cost of Ownership (TCO) by reducing the need to invest in large capital expenditures and providing a pay-as-you-go model that empowers to invest in the capacity you need and use it only when the business requires it. Once you describe your on-premises or hosting environment configuration, it produces a detailed cost comparison with AWS.  
AWS Cost Explorer – AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and gives you a detailed breakdown of all services in the table view. The reports let you adjust the time range to view historical data going back up to twelve months to gain an understanding of your cost trends. AWS Cost Explorer cannot provide a detailed report of your AWS costs by the hour into an S3 bucket.  
AWS Budgets – AWS Budgets gives the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Budgets can be created at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. AWS Budgets cannot provide the estimate of the monthly AWS bill based on the list of AWS services. AWS Budgets cannot provide a detailed break down of your AWS costs by the hour.  
Exam Alert:  
Please review the differences between “AWS Cost and Usage Reports” and “AWS Cost Explorer”. Think of “AWS Cost and Usage Reports” as a cost management tool providing the most detailed cost and usage data for your AWS account. It can provide reports that break down your costs by the hour into your S3 bucket. On the other hand, “AWS Cost Explorer” is more of a high-level cost management tool that helps you visualize the costs and usage associated with your AWS account.  
“AWS Cost Explorer” vs “AWS Cost and Usage Reports”:  via – https://aws.amazon.com/aws-cost-management/aws-cost-explorer/  
 via – https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/  
References:  
<https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html>  
<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>  
<https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/>

**29. Question**

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

* + **Cost Optimization**
  + **Service Limits**
  + Change Management
  + Documentation
  + Elasticity

**Unattempted**

Correct options:  
Cost Optimization  
Service Limits  
AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor on a regular basis help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.  
How Trusted Advisor Works:  via – https://aws.amazon.com/premiumsupport/technology/trusted-advisor/  
AWS Trusted Advisor Recommendations:  via – https://aws.amazon.com/premiumsupport/technology/trusted-advisor/  
Incorrect options:  
Elasticity  
Documentation  
Change Management  
These three options are made-up and have no importance in the context of AWS Trusted Advisor.  
Reference:  
<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

**30. Question**

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

* + Amazon Elastic Container Registry (ECR)
  + AWS Fargate
  + AWS Lambda
  + **Amazon Elastic Container Service (Amazon ECS)**

**Unattempted**

Correct option:  
Amazon Elastic Container Service (Amazon ECS) – Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster. This is not a fully managed service and you can manage the underlying servers yourself.  
Incorrect options:  
AWS Fargate – AWS Fargate is a serverless compute engine for containers. It works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. With Fargate, you do not have access to the underlying servers, so this option is incorrect.  
How Fargate Works:  via – https://aws.amazon.com/fargate/  
AWS Lambda – AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. Lambda does not support running container applications.  
Amazon Elastic Container Registry (ECR) – Amazon Elastic Container Registry (ECR) can be used to store, manage, and deploy Docker container images. Amazon ECR eliminates the need to operate your container repositories. ECR does not support running container applications.  
Reference:  
<https://aws.amazon.com/fargate/>

**31. Question**

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

* + **Enable MFA for all users**
  + Share AWS account root user access keys with other administrators
  + Grant maximum privileges to avoid assigning privileges again
  + Create a minimum number of accounts and share these account credentials among employees
  + **Rotate credentials regularly**

**Unattempted**

Correct option:  
Enable MFA for all users – AWS recommends that you require multi-factor authentication (MFA) for all users in your account. With MFA, users have a device that generates a response to an authentication challenge. Both the user’s credentials and the device-generated response are required to complete the sign-in process.  
Rotate credentials regularly – AWS recommends that you change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a password policy to your account to require all your IAM users to rotate their passwords.  
AWS IAM security best practices:  via – https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html  
Incorrect options: Create a minimum number of accounts and share these account credentials among employees – AWS recommends that user account credentials should not be shared between users.  
Grant maximum privileges to avoid assigning privileges again – AWS recommends granting the least privileges required to complete a certain job and avoid giving excessive privileges which can be misused.  
Share AWS account root user access keys with other administrators – The access key for your AWS account root user gives full access to all your resources for all AWS services, including your billing information. You cannot reduce the permissions associated with your AWS account root user access key. You should never share these access keys with any other users, not even the administrators.  
Reference:  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

**32. Question**

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

* + Elasticity
  + Ability to deploy globally in minutes
  + **Agility**
  + Cost savings

**Unattempted**

Correct option:  
Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS).  
Agility – Agility refers to the ability of the cloud to give you easy access to a broad range of technologies so that you can innovate faster and build nearly anything that you can imagine. You can quickly spin up resources as you need them – from infrastructure services, such as compute, storage, and databases, to Internet of Things, machine learning, data lakes and analytics, and much more.  
Incorrect options:  
Elasticity – With cloud computing elasticity, you don’t have to over-provision resources upfront to handle peak levels of business activity in the future. Instead, you provision the number of resources that you actually need. You can scale these resources up or down instantly to grow and shrink capacity as your business needs change.  
Cost savings – The cloud allows you to trade capital expenses (such as data centers and physical servers) for variable expenses, and only pay for IT as you consume it. Plus, the variable expenses are much lower than what you would pay to do it yourself because of the economies of scale.  
Ability to deploy globally in minutes – With the cloud, you can expand to new geographic regions and deploy globally in minutes. For example, AWS has infrastructure all over the world, so you can deploy your application in multiple physical locations with just a few clicks. Putting applications in closer proximity to end users reduces latency and improves their experience.  
Exam Alert:  
Please review the benefits of Cloud Computing:   
 via – https://aws.amazon.com/what-is-cloud-computing/  
Reference:  
<https://aws.amazon.com/what-is-cloud-computing/>

**33. Question**

Which pillar of the AWS Well-Architected Framework recommends monitoring your application’s performance?

* + Security
  + Reliability
  + Operational Excellence
  + **Performance Efficiency**

**Unattempted**

Correct option:  
Performance Efficiency  
The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement.  
The AWS Well-Architected Framework is based on five pillars — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.  
The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.  
After you have implemented your architecture you will need to monitor its performance so that you can remediate any issues before your customers are aware. Monitoring metrics should be used to raise alarms when thresholds are breached.  
Incorrect options:  
Reliability – The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross-project requirements, recovery planning, and how we handle change.  
Operational Excellence – The Operational Excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events.  
Security – The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.  
Reference:  
<https://wa.aws.amazon.com/wat.pillar.performance.en.html>

**34. Question**

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

* + **Spot Instance**
  + Dedicated Host
  + Reserved Instance
  + On-Demand Instance

**Unattempted**

Correct option:  
Spot Instance – A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts (up to 90%), you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and other flexible tasks that can be interrupted. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time.  
EC2 Pricing Options Overview:  via – https://aws.amazon.com/ec2/pricing/  
Incorrect options:  
On-Demand Instance – An On-Demand Instance is an instance that you use on-demand. You have full control over its lifecycle — you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you pay only for the seconds that your On-Demand Instances are running. The price per second for running an On-Demand Instance is fixed. On-demand instances cannot be interrupted. However, On-demand instances are not as cost-effective as spot instances, so this option is not correct.  
Reserved Instance – Reserved Instances provide you with significant savings (up to 75%) on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a one-year or three-year commitment, with the three-year commitment offering a bigger discount. Reserved instances cannot be interrupted. Reserved instances are not as cost-effective as spot instances, so this option is not correct.  
Dedicated Host – Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2 so that you get the flexibility and cost-effectiveness of using your licenses, but with the resiliency, simplicity, and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirement. They’re not cost-efficient compared to spot instances. So this option is not correct.  
Reference:  
<https://aws.amazon.com/ec2/pricing/>

**35. Question**

Which of the following AWS services are regional in scope? (Select two)

* + **Amazon Rekognition**
  + AWS Identity and Access Management (IAM)
  + Amazon CloudFront
  + **AWS Lambda**
  + AWS WAF

**Unattempted**

Correct options:  
Most of the services that AWS offers are Region specific. But few services, by definition, need to be in a global scope because of the underlying service they offer. AWS IAM, Amazon CloudFront, Route 53 and WAF are some of the global services.  
AWS Lambda – AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. Lambda is a regional service.  
Amazon Rekognition – With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases. Rekognition is a regional service.  
Incorrect options:  
AWS Identity and Access Management (IAM) – AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.  
Amazon CloudFront – Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.  
AWS WAF – By using AWS WAF, you can configure web access control lists (Web ACLs) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures.  
As mentioned earlier, these three services are global in scope.  
Exam Alert:  
Amazon S3 – Amazon S3 is a unique service in the sense that it follows a global namespace but the buckets are regional. You specify an AWS Region when you create your Amazon S3 bucket. This is a regional service.

**36. Question**

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

* + **AWS Transit Gateway**
  + VPC Peering
  + AWS Direct Connect
  + Site to Site VPN

**Unattempted**

Correct option:  
AWS Transit Gateway  
AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. As you expand globally, inter-Region peering connects AWS Transit Gateways using the AWS global network. Your data is automatically encrypted and never travels over the public internet.  
How Transit Gateway can simplify your network:  via – https://aws.amazon.com/transit-gateway/  
Incorrect options:  
VPC Peering – A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. VPC peering is not transitive, a separate VPC peering connection has to be made between two VPCs that need to talk to each other. With growing VPCs, this gets difficult to manage.  
Transitive VPC Peering is not allowed:  via – https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html  
AWS Direct Connect – AWS Direct Connect creates a dedicated private connection from a remote network to your VPC. This is a private connection and does not use the public internet. Takes at least a month to establish this connection. Direct Connect cannot be used to interconnect VPCs.  
Site to Site VPN – AWS Site-to-Site VPN creates a secure connection between your data center or branch office and your AWS cloud resources. This connection goes over the public internet. Site to Site VPN cannot be used to interconnect VPCs.  
Reference:  
<https://aws.amazon.com/transit-gateway/>

**37. Question**

Which AWS service can be used for online analytical processing?

* + Amazon ElastiCache
  + Amazon RDS
  + **Amazon Redshift**
  + Amazon DynamoDB

**Unattempted**

Correct option:  
Amazon Redshift  
Amazon Redshift is a fast, fully managed cloud data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It allows you to run complex analytic queries against terabytes to petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution.  
Incorrect options:  
Amazon RDS – Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups.  
Customers use Amazon RDS databases primarily for online-transaction processing (OLTP) workload while Redshift is used primarily for reporting and analytics.  
Amazon DynamoDB – Amazon DynamoDB is a NoSQL database that supports key-value and document data models and enables developers to build modern, serverless applications that can start small and scale globally to support petabytes of data and tens of millions of read and write requests per second. DynamoDB supports both key-value and document data models. This enables DynamoDB to have a flexible schema, so each row can have any number of columns at any point in time. This allows you to easily adapt the tables as your business requirements change, without having to redefine the table schema as you would in relational databases. DynamoDB cannot be used for online analytical processing.  
Amazon ElastiCache – Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-Source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for real-time use cases like Caching, Session Stores, Gaming, Geospatial Services, Real-Time Analytics, and Queuing. ElastiCache cannot be used for online analytical processing.  
Reference:  
<https://aws.amazon.com/redshift/faqs/>

**38. Question**

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

* + Amazon Redshift
  + Amazon EBS volumes
  + Amazon EFS drives
  + **AWS Storage Gateway**
  + **Amazon S3 Glacier**

**Unattempted**

Correct option:  
Amazon S3 Glacier – Amazon S3 Glacier (S3 Glacier), is a storage service optimized for infrequently used data, or “cold data. Data at rest stored in S3 Glacier is automatically server-side encrypted using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS.  
AWS Storage Gateway – AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways – File, Volume and Tape Gateways).  
Incorrect options:  
Amazon EBS volumes – Amazon EBS volumes are not encrypted, by default. You can configure your AWS account to enforce the encryption of the new EBS volumes and snapshot copies that you create.  
Amazon Redshift – Encryption is an optional setting in Amazon Redshift. When you enable encryption for a cluster, the data-blocks and system metadata are encrypted for the cluster and its snapshots.  
Amazon EFS drives – Encryption is not a default setting, but an optional configuration for EFS drives. Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest.  
References:  
<https://aws.amazon.com/storagegateway/faqs/>  
<https://docs.aws.amazon.com/amazonglacier/latest/dev/DataEncryption.html>

**39. Question**

Which S3 storage class offers the lowest availability?

* + S3 Glacier
  + **S3 One Zone-IA**
  + S3 Intelligent-Tiering
  + S3 Standard

**Unattempted**

Correct option:  
S3 One Zone-IA  
S3 One Zone-IA is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ.  
Please review this illustration for S3 Storage Classes availability. You don’t need to memorize the actual numbers, just remember that S3 One Zone-IA offers the lowest availability:  via – https://aws.amazon.com/s3/storage-classes/  
Incorrect options:  
S3 Standard – S3 Standard offers high durability, availability, and performance object storage for frequently accessed data.  
S3 Intelligent-Tiering – The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access.  
S3 Glacier – Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.  
References:  
<https://aws.amazon.com/s3/storage-classes/>

**40. Question**

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

* + **Amazon Simple Storage Service (Amazon S3)**
  + AWS Elastic Beanstalk
  + Amazon Elastic Compute Cloud (Amazon EC2)
  + AWS Storage Gateway

**Unattempted**

Correct option:  
Amazon Simple Storage Service (Amazon S3)  
Software as a Service (SaaS) provides you with a complete product that is run and managed by the service provider. With a SaaS offering, you don’t have to think about how the service is maintained or how the underlying infrastructure is managed. You only need to think about how you will use that particular software.  
Amazon Simple Storage Service (Amazon S3) – Amazon S3 can be used for storing data directly without having to do anything with underlying infrastructure, maintenance or deployments. S3 is an example of a storage service that can be categorized as Software as a Service (SaaS).  
Overview of Cloud Computing Types:  via – https://aws.amazon.com/types-of-cloud-computing/  
Incorrect options:  
Infrastructure as a Service (IaaS) contains the basic building blocks for cloud IT. It typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS gives the highest level of flexibility and management control over IT resources.  
Platform as a Service (PaaS) removes the need to manage underlying infrastructure (usually hardware and operating systems), and allows you to focus on the deployment and management of your applications. You don’t need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.  
Amazon Elastic Compute Cloud (Amazon EC2) – Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. EC2 provides compute capacity and maintenance of guest Operating systems, patches and deployment of code is the responsibility of the customer. So, EC2 comes under Infrastructure as a Service (IaaS).  
AWS Storage Gateway – AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. You use the AWS Management Console to download the virtual appliance gateway or purchase the hardware appliance, hence it does not fall under Software as a Service model.  
\*AWS Elastic Beanstalk \* – AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with a wide range of programming languages. You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. This service falls under Platform as a Service (PaaS).  
Reference:  
<https://aws.amazon.com/what-is-cloud-computing/>

**41. Question**

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

* + AWS Direct Connect
  + AWS Transit Gateway
  + **AWS Snowball**
  + AWS Virtual Private Network (VPN)

**Unattempted**

Correct option:  
AWS Snowball  
AWS Snowball, a part of the AWS Snow Family, is a data migration and edge computing device. If you have large quantities of data you need to migrate into AWS, offline data transfer with AWS Snowball can overcome the challenge of limited bandwidth, and avoid the need to lease additional bandwidth. Snowball moves terabytes of data in about a week. You can use it to move things like databases, backups, archives, healthcare records, analytics datasets, IoT sensor data and media content, especially when network conditions prevent realistic timelines for transferring large amounts of data both into and out of AWS.  
Incorrect options:  
AWS Virtual Private Network (VPN) – A VPN connection refers to the connection between your Virtual Private Cloud and your on-premises network. By default, instances that you launch into an Amazon VPC can’t communicate with your own (remote) network. You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection, and configuring routing to pass traffic through the connection. VPN aids regular connectivity of AWS and your private om-premises network, it is not a data migration solution.  
AWS Direct Connect – AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you with a private, high bandwidth network connection between your network and your VPC. This connection is private and does not go over the public internet. It takes at least a month to establish this physical connection. It is not feasible to set up AWS Direct Connect in remote locations.  
AWS Transit Gateway – AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. VPC peering across large connections is made possible using Transit Gateway without ending up with a complex VPC peering network. Transit Gateway is not a data migration solution.  
Reference:  
<https://aws.amazon.com/snowball/>

**42. Question**

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

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

**Unattempted**

Correct option:  
You must use an AMI from the same region as that of the EC2 instance. The region of the AMI has no bearing on the performance of the EC2 instance  
An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration.  
The AMI must be in the same region as that of the EC2 instance to be launched. If the AMI exists in a different region, you can copy that AMI to the region where you want to launch the EC2 instance. The region of AMI has no bearing on the performance of the EC2 instance.  
Amazon Machine Images (AMI) Overview:  via – https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html  
Incorrect options:  
You can use an AMI from a different region, but it degrades the performance of the EC2 instance  
You should use an AMI from the same region, as it improves the performance of the EC2 instance  
An AMI is a global entity, so the region is not applicable  
These three options contradict the details provided earlier in the explanation, so these options are incorrect.  
Reference:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

**43. Question**

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

* + **You must activate both AWS generated tags and user-defined tags separately before they can appear in Cost Explorer or on a cost allocation report**
  + Tags helps in organizing resources and are a mandatory configuration item to run reports
  + For each resource, each tag key must be unique, but can have multiple values
  + Only user-defined tags need to be activated before they can appear in Cost Explorer or on a cost allocation report
  + **For each resource, each tag key must be unique, and each tag key can have only one value**

**Unattempted**

Correct options:  
For each resource, each tag key must be unique, and each tag key can have only one value  
You must activate both AWS generated tags and user-defined tags separately before they can appear in Cost Explorer or on a cost allocation report  
A Cost Allocation Tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. For each resource, each tag key must be unique, and each tag key can have only one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level.  
AWS provides two types of cost allocation tags, an AWS generated tags and user-defined tags. AWS defines, creates, and applies the AWS generated tags for you, and you define, create, and apply user-defined tags. You must activate both types of tags separately before they can appear in Cost Explorer or on a cost allocation report.  
AWS Cost Allocation Tags Overview:  via – https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html  
Incorrect options:  
Tags helps in organize resources and are a mandatory configuration item to run reports – Tags definitely help organize resources as per an organization’s requirement; they are not mandatory though.  
For each resource, each tag key must be unique, but can have multiple values – For each resource, each tag key must be unique, and each tag key can have only one value.  
Only user-defined tags need to be activated before they can appear in Cost Explorer or on a cost allocation report – As explained above, both kinds of tags (user-defined and AWS generated) need to be activated separately before they can appear in report generation.  
Reference:  
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html>

**44. Question**

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

* + **The time it takes for the lambda function to execute**
  + The number of lines of code for the lambda function
  + The language runtime of the lambda function
  + **Number of requests for the lambda function**
  + The size of the deployment package for the lambda function

**Unattempted**

Correct options:  
Number of requests for the lambda function  
The time it takes for the lambda function to execute  
AWS Lambda lets you run code without provisioning or managing servers. With Lambda, you can run code for virtually any type of application or backend service – all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability.  
With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the duration, the time it takes for your code to execute. Lambda counts a request each time it starts executing in response to an event notification or invoke call, including test invokes from the console. Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms.  
Incorrect options:  
The language runtime of the lambda function – Lambda supports many programming language runtimes such as NodeJS, Python, Go, C# etc. The pricing for a lambda function is not dependent on the language runtime of the lambda function.  
The number of lines of code for the lambda function – The pricing for a lambda function is not dependent on the number of lines of code for the lambda function.  
The size of the deployment package for the lambda function – The pricing for a lambda function is not dependent on the size of the deployment package for the lambda function.  
Reference:  
<https://aws.amazon.com/lambda/pricing/>

**45. Question**

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

* + **AWS Trusted Advisor**
  + Amazon CloudWatch
  + AWS Cost Explorer
  + AWS Cost and Usage Reports

**Unattempted**

Correct option:  
AWS Trusted Advisor  
AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.  
AWS Trusted Advisor checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days.  
How Trusted Advisor Works:  via – https://aws.amazon.com/premiumsupport/technology/trusted-advisor/  
How AWS Trusted Advisor identifies low utilization Amazon EC2 instances:  via – https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/#Cost\_Optimization  
Incorrect options:  
AWS Cost Explorer – AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and gives you a detailed breakdown of all services in the table view. The reports let you adjust the time range to view historical data going back up to twelve months to gain an understanding of your cost trends. Cost Explorer cannot be used to identify under-utilized EC2 instances.  
AWS Cost and Usage Reports – The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself. Cost and Usage Reports cannot be used to identify under-utilized EC2 instances.  
Amazon CloudWatch – Amazon CloudWatch can be used to create alarm to monitor your estimated charges. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data. You can choose to receive alerts by email when charges have exceeded a certain threshold. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot be used to identify under-utilized EC2 instances.  
Reference:  
<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/#Cost_Optimization>

##### **46. Question**

An AWS hardware failure has impacted one of your EBS volumes. Which AWS service will alert you of the affected resources and provide a remedial action?

* + **AWS Personal Health Dashboard**
  + AWS Trusted Advisor
  + Amazon GuardDuty
  + AWS Config

**Unattempted**

Correct option:  
AWS Personal Health Dashboard  
AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view of the performance and availability of the AWS services underlying your AWS resources. The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues. For example, in the event of an AWS hardware failure impacting one of your EBS volumes, you will get an alert that includes a list of your affected resources, a recommendation to restore your volume, and links to the steps to help you restore it from a snapshot.  
Incorrect options:  
Amazon GuardDuty – Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns).  
AWS Config – AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.  
AWS Trusted Advisor – AWS Trusted Advisor is an online tool that provides real-time guidance to help you provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor on a regular basis help keep your solutions provisioned optimally.  
Reference:  
<https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/>

**47. Question**

Which of the following is correct regarding the AWS Shield Advanced pricing?

* + AWS Shield Advanced is a free service for all AWS Support plans
  + **AWS Shield Advanced offers protection against higher fees that could result from a DDoS attack**
  + AWS Shield Advanced is a free service for AWS Enterprise Support plan
  + AWS Shield Advanced is a free service for AWS Business Support plan

**Unattempted**

Correct option:  
AWS Shield Advanced offers protection against higher fees that could result from a DDoS attack  
AWS Shield Advanced offers some cost protection against spikes in your AWS bill that could result from a DDoS attack. This cost protection is provided for your Elastic Load Balancing load balancers, Amazon CloudFront distributions, Amazon Route 53 hosted zones, Amazon Elastic Compute Cloud instances, and your AWS Global Accelerator accelerators.  
AWS Shield Advanced is a paid service for all customers, irrespective of the Support plan.  
Incorrect options:  
AWS Shield Advanced is a free service for AWS Enterprise Support plan  
AWS Shield Advanced is a free service for AWS Business Support plan  
AWS Shield Advanced is a free service for all AWS Support plans  
These three options contradict the details provided earlier in the explanation, so these options are incorrect.  
Reference:  
<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html>

**48. Question**

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

* + **Create separate AWS accounts for development and production environments to receive separate invoices**
  + Use AWS Cost Explorer to create separate invoices for development and production environments
  + Tag all resources in the AWS account as either "development" or "production". Then use the tags to create separate invoices
  + Use AWS Organizations to create separate invoices for development and production environments

**Unattempted**

Correct option:  
“Create separate AWS accounts for development and production environments to receive separate invoices”  
Every AWS account provides its own invoice end of the month. You can get separate invoices for development and production environments by setting up separate AWS accounts for each environment.  
Incorrect options:  
Use AWS Organizations to create separate invoices for development and production environments – AWS Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts. Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance. You can also simplify billing by setting up a single payment method for all of your AWS accounts. AWS Organizations is available to all AWS customers at no additional charge.  
AWS Organizations cannot create separate invoices for development and production environments, rather, AWS Organizations helps you to centrally manage billing.  
Tag all resources in the AWS account as either “development” or “production”. Then use the tags to create separate invoices – You cannot create separate invoices based on tags.  
“Use AWS Cost Explorer to create separate invoices for development and production environments” – AWS Cost Explorer lets you explore your AWS costs and usage at both a high level and at a detailed level of analysis, and empowering you to dive deeper using several filtering dimensions (e.g., AWS Service, Region, Linked Account). AWS Cost Explorer cannot create separate invoices for development and production environments.  
Reference:  
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html>

**49. Question**

Which of the following AWS entities provides the information required to launch an EC2 instance?

* + **AMI**
  + EFS
  + EBS
  + Lambda

**Unattempted**

Correct option:  
AMI  
An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance.  
An AMI includes the following:  
One or more EBS snapshots, or, for instance-store-backed AMIs, a template for the root volume of the instance (for example, an operating system, an application server, and applications).  
Launch permissions that control which AWS accounts can use the AMI to launch instances.  
A block device mapping that specifies the volumes to attach to the instance when it’s launched.  
The following diagram summarizes the AMI lifecycle:  via – https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html  
Incorrect options:  
Lambda – AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume.  
EFS – Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.  
EBS – Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale.  
Reference:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>

**50. Question**

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

* + Use CloudTrail for the EC2 instance and CloudWatch Logs for the on-premises servers
  + Use AWS Lambda to send log data from EC2 instance as well as on-premises servers to CloudWatch Logs
  + **Use CloudWatch Logs for both the EC2 instance and the on-premises servers**
  + Use CloudWatch Logs for the EC2 instance and CloudTrail for the on-premises servers

**Unattempted**

Correct option:  
Use CloudWatch Logs for both the EC2 instance and the on-premises servers  
You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources such as on-premises servers.  
CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis.  
Incorrect options:  
Use AWS Lambda to send log data from EC2 instance as well as on-premises servers to CloudWatch Logs  
AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Lambda cannot be used to centralize the logs from EC2 instances and on-premises servers.  
Use CloudWatch Logs for the EC2 instance and CloudTrail for the on-premises servers  
Use CloudTrail for the EC2 instance and CloudWatch Logs for the on-premises servers  
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. CloudTrail cannot be used to centralize the server logs for EC2 instances or on-premises servers, so both these options are incorrect.  
References:  
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>  
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html>

**51. Question**

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

* + AWS CloudTrail
  + Amazon GuardDuty
  + **AWS Config**
  + Amazon Macie

**Unattempted**

Correct option:  
AWS Config  
AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time. AWS Config is designed to help you oversee your application resources in the following scenarios: Resource Administration, Auditing and Compliance, Managing and Troubleshooting Configuration Changes, Security Analysis.  
How AWS Config Works:  via – https://aws.amazon.com/config/  
Incorrect options:  
Amazon Macie – Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII). This service is an added security feature for data privacy and is not the best fit for the current requirement.  
AWS CloudTrail – AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides an event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services.  
Config is focused on the configuration of your AWS resources and reports with detailed snapshots on how your resources have changed. Whereas CloudTrail focuses on the events or API calls, that drive those changes. It focuses on the user, application, and activity performed on the system.  
Amazon GuardDuty – Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail, Amazon VPC Flow Logs, and DNS Logs. Its a threat detection service and not a configuration management and tracking service.  
References:  
<https://aws.amazon.com/config/>  
<https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>

**52. Question**

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

* + EFS
  + **Instance Store**
  + ECS
  + S3
  + **EBS**

**Unattempted**

Correct options:  
EBS – Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.  
Instance Store – An instance store provides temporary block-level storage for your EC2 instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance storage is temporary, data is lost if instance experiences failure or is terminated. EC2 instance store cannot be used for file sharing between instances.  
Incorrect options:  
EFS – Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS file system. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.  
S3 – Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics.  
ECS – Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. This is not a storage service and has been added as a distractor.  
References:  
<https://aws.amazon.com/ebs/>  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

**53. Question**

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

* + Auto Scaling group scales up and upgrades to a more powerful EC2 instance to match an increase in demand
  + Auto Scaling group scales down and downgrades to a less powerful EC2 instance to match a decrease in demand
  + **Auto Scaling group scales out and adds more number of EC2 instances to match an increase in demand**
  + **Auto Scaling group scales in and reduces the number of EC2 instances to match a decrease in demand**
  + Auto Scaling group scales down and reduces the number of EC2 instances to match a decrease in demand

**Unattempted**

Correct option:  
Auto Scaling group scales out and adds more number of EC2 instances to match an increase in demand  
Auto Scaling group scales in and reduces the number of EC2 instances to match a decrease in demand  
AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it’s easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas.  
You can use scaling policies to increase or decrease the number of instances in your group dynamically to meet changing conditions. When the scaling policy is in effect, the Auto Scaling group adjusts the desired capacity of the group, between the minimum and maximum capacity values that you specify, and launches or terminates the instances as needed. You can also scale on a schedule.  
Incorrect options:  
Auto Scaling group scales down and reduces the number of EC2 instances to match a decrease in demand – A scale down refers to a downgrade to a less powerful EC2 instance. Therefore this option is incorrect.  
Auto Scaling group scales down and downgrades to a less powerful EC2 instance to match a decrease in demand  
Auto Scaling group scales up and upgrades to a more powerful EC2 instance to match an increase in demand  
An Auto Scaling group does not scale up or scale down, so these two options are incorrect.  
Reference:  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

**54. Question**

Which AWS Support plan guarantees a case response time of 15 minutes when Business Critical systems are down?

* + Business
  + Developer
  + **Enterprise**
  + Basic

**Unattempted**

Correct option:  
Enterprise – AWS Enterprise Support provides customers with concierge-like service where the main focus is helping the customer achieve their outcomes and find success in the cloud. With Enterprise Support, you get 24×7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative architectural guidance delivered in the context of your applications and use-cases, and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts. This plan provides Enhanced Technical Support as follows:  
24×7 access to Cloud Support Engineers via phone, chat, and email. You can have an unlimited number of contacts that can open an unlimited amount of cases. Response times are as follows:  
General Guidance – < 24 hours System Impaired - < 12 hours Production System Impaired - < 4 hours Production System Down - < 1 hour Business Critical System Down - <15 min Benefits of AWS Enterprise Support Plan:  via - https://aws.amazon.com/premiumsupport/plans/enterprise/ Incorrect options: Business - AWS recommends Business Support if you have production workloads on AWS and want 24x7 phone, email, and chat access to technical support and architectural guidance in the context of your specific use-cases. You get full access to AWS Trusted Advisor Best Practice Checks. This plan does not guarantee any specific response time for Business Critical systems. Developer - AWS recommends Developer Support if you are testing or doing early development on AWS and want the ability to get email-based technical support during business hours as well as general architectural guidance as you build and test. You do not get access to Infrastructure Event Management with this plan. This plan does not guarantee any specific response time for Business Critical systems. Basic - The basic plan only provides access to the following: Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted. This plan does not guarantee any specific response time for Business Critical systems. Reference: <https://aws.amazon.com/premiumsupport/plans/enterprise/>

**55. Question**

Which of the following improves the availability for a fleet of EC2 instances?

* + Deploy the EC2 instances across different AWS Regions of the same Availability Zone
  + Deploy the EC2 instances in the same Availability Zone across two different AWS Regions
  + **Deploy the EC2 instances across different Availability Zones in the same AWS Region**
  + Deploy the EC2 instances in the same Availability Zone of an AWS Region

**Unattempted**

Correct option:  
Deploy the EC2 instances across different Availability Zones in the same AWS Region  
AWS has the concept of a Region, which is a physical location around the world where AWS clusters data centers. Each AWS Region consists of multiple (two or more), isolated, and physically separate AZ’s within a geographic area. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks.  
An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. An AWS Region refers to a physical location around the world where AWS clusters data centers. AZ’s give customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data center. All AZ’s in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber providing high-throughput, low-latency networking between AZ’s.  
AWS Regions and Availability Zones Explained:  via – https://aws.amazon.com/about-aws/global-infrastructure/regions\_az/  
Incorrect options:  
Deploy the EC2 instances in the same Availability Zone of an AWS Region – Deploying EC2 instances within the same AZ will not improve availability.  
Deploy the EC2 instances in the same Availability Zone across two different AWS Regions – An Availability Zone cannot belong to two different AWS Regions. So this option is incorrect.  
Deploy the EC2 instances across different AWS Regions of the same Availability Zone – You cannot have an AWS Region inside an Availability Zone. So this option is incorrect.  
Reference:  
<https://aws.amazon.com/about-aws/global-infrastructure/regions_az/>

**56. Question**

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

* + S3 One Zone-IA
  + S3 Standard
  + **S3 Glacier**
  + S3 Intelligent-Tiering

**Unattempted**

Correct option:  
S3 Glacier  
Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.  
You can further review the use-cases for S3 Glacier:  via – https://aws.amazon.com/glacier/  
S3 Storage Classes Overview:  via – https://aws.amazon.com/s3/storage-classes/  
Incorrect options:  
S3 Standard – S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. It is not suitable for data archival.  
S3 Intelligent-Tiering – The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. It is not suitable for data archival.  
S3 One Zone-IA – S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ. It is not suitable for data archival.  
References:  
<https://aws.amazon.com/glacier/>  
<https://aws.amazon.com/s3/storage-classes/>

**57. Question**

Which AWS service protects your AWS account by monitoring malicious activity and detecting threats?

* + CloudTrail
  + Trusted Advisor
  + CloudWatch
  + **GuardDuty**

**Unattempted**

Correct option:  
GuardDuty  
GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). Security findings are retained and made available through the Amazon GuardDuty console and APIs for 90-days. After 90-days, the findings are discarded. To retain findings for longer than 90-days, you can enable AWS CloudWatch Events to automatically push findings to an Amazon S3 bucket in your account or another data store for long-term retention.  
How GuardDuty Works:  via – https://aws.amazon.com/guardduty/  
Incorrect options:  
CloudTrail – AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Think account-specific activity and audit; think CloudTrail. CloudTrail cannot detect threats to your AWS account.  
CloudWatch – Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Think resource performance monitoring, events, and alerts; think CloudWatch. CloudWatch cannot detect threats to your AWS account.  
Trusted Advisor – AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. Trusted Advisor cannot detect threats to your AWS account.  
Reference:  
<https://aws.amazon.com/guardduty>

**58. Question**

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

* + **75**
  + 90
  + 40
  + 50

**Unattempted**

Correct option:  
75  
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.  
EC2 Pricing Options Overview:  via – https://aws.amazon.com/ec2/pricing/  
Incorrect options:  
90  
50  
40  
60  
Reference:  
<https://aws.amazon.com/ec2/pricing/>

**59. Question**

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

* + For every new object, trigger a lambda function to write data into a bucket in another AWS Region
  + **Use Cross-Region replication (CRR) to replicate data between distant AWS Regions**
  + Use Same-Region replication (SRR) to replicate data between distant AWS Regions
  + Run a daily job on an EC2 instance to copy objects into another Region

**Unattempted**

Correct option:  
Use Cross-Region replication (CRR) to replicate data between distant AWS Regions  
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.  
Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region.  
Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-Region Replication (CRR) allows you to replicate data between distant AWS Regions to satisfy these requirements.  
Incorrect options:  
Use Same-Region replication (SRR) to replicate data between distant AWS Regions – SRR is used to copy objects across Amazon S3 buckets in the same AWS Region, so this option is incorrect.  
Exam Alert:  
Please review the differences between SRR and CRR:  via – https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html  
For every new object, trigger a lambda function to write data into a bucket in another AWS Region – Although this solution is feasible, it’s not resource efficient as the lambda is used to do something which S3 CRR can achieve off-the-shelf.  
Run a daily job on an EC2 instance to copy objects into another Region – Creating a daily job on EC2 instance to copy objects into another Region involves a lot of development effort. It is much better to use S3 CRR for this task.  
Reference:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html>

**60. Question**

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

* + **Virtual Private Gateway**
  + Storage Gateway
  + **Customer Gateway**
  + NAT Gateway
  + Internet Gateway

**Unattempted**

Correct option:  
Virtual Private Gateway  
Customer Gateway  
AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). VPN Connections are a good solution if you have an immediate need, and have low to modest bandwidth requirements. This connection goes over the public internet. Virtual Private Gateway (or a Transit Gateway) and Customer Gateway are the components of a VPC.  
A virtual private gateway is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. A customer gateway is a resource in AWS that provides information to AWS about your Customer gateway device.  
Components of an AWS Site-to-Site VPN:  via – https://docs.aws.amazon.com/vpn/latest/s2svpn/how\_it\_works.html  
Incorrect options:  
Storage Gateway – AWS Storage Gateway is a hybrid cloud storage service that connects your existing on-premises environments with the AWS Cloud. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases.  
NAT Gateway – A NAT Gateway or a NAT Instance can be used in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet. NAT Gateway is managed by AWS but NAT Instance is managed by you.  
Internet Gateway – An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It, therefore, imposes no availability risks or bandwidth constraints on your network traffic.  
Reference:  
<https://docs.aws.amazon.com/vpn/latest/s2svpn/how_it_works.html>

**61. Question**

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

* + Public Cloud
  + **Hybrid Cloud**
  + Private Cloud
  + On-premises

**Unattempted**

Correct option:  
Hybrid Cloud  
A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud. The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend, and grow, an organization’s infrastructure into the cloud while connecting cloud resources to the internal system.  
Overview of Cloud Computing Deployment Models:  via – https://aws.amazon.com/types-of-cloud-computing/  
Incorrect options:  
Public Cloud – A public cloud-based application is fully deployed in the cloud and all parts of the application run in the cloud. Applications in the cloud have either been created in the cloud or have been migrated from an existing infrastructure to take advantage of the benefits of cloud computing.  
Private Cloud – Unlike a Public cloud, a Private cloud enables businesses to avail IT services that are provisioned and customized according to their precise needs. The business can further avail the IT services in a secure and reliable way over a private IT infrastructure.  
On-premises – This is not a cloud deployment model. When an enterprise opts for on-premises,it needs to create, upgrade, and scale the on-premise IT infrastructure by investing in sophisticated hardware, compatible software, and robust services. Also, the business needs to deploy dedicated IT staff to upkeep, scale, and manage the on-premise infrastructure continuously.  
Reference:  
<https://aws.amazon.com/what-is-cloud-computing/>

**62. Question**

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

* + Network Stress Testing
  + **Penetration Testing**
  + AWS Secrets Manager
  + Amazon Inspector

**Unattempted**

Correct option:  
Penetration Testing  
AWS customers can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for few common AWS services. Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves.  
Incorrect options:  
Network Stress Testing – AWS considers “network stress test” to be when a test sends a large volume of legitimate or test traffic to a specific intended target application. The endpoint and infrastructure are expected to be able to handle this traffic.  
Amazon Inspector – Amazon Inspector is an automated, security assessment service that helps you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.  
AWS Secrets Manager – AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.  
Reference:  
<https://aws.amazon.com/security/penetration-testing/>

**63. Question**

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

* + **For abstracted services like Amazon S3, AWS operates the infrastructure layer, the operating system, and platforms**
  + Configuration Management is the responsibility of the customer
  + **AWS is responsible for Security "of" the Cloud**
  + For a service like Amazon EC2, that falls under Infrastructure as a Service, AWS is responsible for maintaining guest operating system
  + AWS is responsible for training AWS and customer employees on AWS products and services

**Unattempted**

Correct options:  
Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer’s operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.  
AWS is responsible for Security “of” the Cloud – AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.  
“For abstracted services like Amazon S3, AWS operates the infrastructure layer, the operating system, and platforms” – For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data.  
Shared Responsibility Model Overview:  via – https://aws.amazon.com/compliance/shared-responsibility-model/  
Incorrect options:  
For a service like Amazon EC2, that falls under Infrastructure as a Service, AWS is responsible for maintaining guest operating system – A service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers are responsible for the management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.  
Configuration Management is the responsibility of the customer – Configuration management is a shared responsibility. AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.  
AWS is responsible for training AWS and customer employees on AWS products and services – Awareness & Training is also a shared responsibility. AWS trains AWS employees, but a customer must train their own employees.  
Reference:  
<https://aws.amazon.com/compliance/shared-responsibility-model/>

**64. Question**

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

* + Latency routing policy
  + Simple routing policy
  + **Failover routing policy**
  + Weighted routing policy

**Unattempted**

Correct option:  
Failover routing policy  
Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like [http://www.example.com](http://www.example.com/) into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other.  
Failover routing policy is used when you want to configure active-passive failover. Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. The primary and secondary records can route traffic to anything from an Amazon S3 bucket that is configured as a website to a complex tree of records.  
Route 53 Routing Policy Overview:  via – https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html  
Incorrect options:  
Simple routing policy – Simple routing lets you configure standard DNS records, with no special Route 53 routing such as weighted or latency. With simple routing, you typically route traffic to a single resource, for example, to a web server for your website.  
Weighted routing policy – This routing policy is used to route traffic to multiple resources in proportions that you specify.  
Latency routing policy – This routing policy is used when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.  
Reference:  
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

**65. Question**

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

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

**Unattempted**

Correct option:  
EC2 instances can access files on an EFS file system across many Availability Zones, regions and VPCs  
Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.  
Amazon EFS Overview:  via – https://aws.amazon.com/efs/  
Incorrect options:  
EC2 instances can access files on an EFS file system only in one Availability Zone  
EC2 instances can access files on an EFS file system across many Availability Zones  
EC2 instances can access files on an EFS file system across many Availability Zones and VPCs  
These three options contradict the details provided earlier in the explanation, so these options are incorrect.  
Reference:  
<https://aws.amazon.com/efs/>