Top of Form

Question 1:

**Skipped**

What is the recommended storage option when hosting an often-changing database on an Amazon EC2 instance?

* 

Amazon DynamoDB

* 

Amazon EBS

**(Correct)**

* 

You can't run a database inside an Amazon EC2 instance

* 

Amazon RDS

**Explanation**

                Amazon EBS provides durable, block-level storage volumes that you can attach to a running EC2 instance. You can use Amazon EBS as a primary storage device for data that requires frequent and granular updates. Amazon EBS is the recommended storage option when you run a database on an EC2 instance.

***The other options are incorrect:***

***"Amazon RDS" is incorrect.***Amazon RDS is not a storage service. Amazon RDS provides AWS-managed databases.

***"You can't run a database inside an Amazon EC2 instance" is incorrect.*** You can install and run any database software you want on Amazon EC2. In this case, you are responsible for managing everything related to this database.

***"Amazon DynamoDB" is incorrect.***Amazon DynamoDB is not a storage service. Amazon DynamoDB is a key-value and document database service.

**References:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

Bottom of Form

Top of Form

Question 2:

**Skipped**

Which statement is true in relation to security in AWS?

* 

AWS is responsible for the security of your application

* 

AWS manages everything related to EC2 operating systems

* 

AWS customers are responsible for patching any database software running on Amazon EC2

**(Correct)**

* 

Server side encryption is the responsibility of AWS

**Explanation**

AWS customers have two options to host their databases on AWS:

1- Using a managed database:

AWS Customers can use managed databases such as Amazon RDS to host their databases. In this case, **AWS is responsible** for performing all database management tasks such as hardware provisioning, patching, setup, configuration, backups, or recovery.

2- Installing a database software on Amazon EC2:

Instead of using a managed database, AWS customers can install any database software they want on Amazon EC2 and host their databases. In this case, **Customers are responsible** for performing all of the necessary configuration and management tasks.

**Note:** For Amazon RDS, all security patches and updates are applied automatically to the database software once they are released. But for databases installed on Amazon EC2, customers are required to apply the security patches and the updates manually or use the AWS Systems Manager service to apply them on a scheduled basis (every week, for example).

***The other options are incorrect:***

***"AWS manages everything related to EC2 operating systems" is incorrect.***It is the responsibility of the customer to choose and manage the operating system.

***"AWS is responsible for the security of your application" is incorrect.*** It is the responsibility of the customer to build secure applications.

***"Server side encryption is the responsibility of AWS" is incorrect.*** It is the responsibility of the customer to encrypt data either on the client side or on the server side.

**References:**

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

Bottom of Form

Top of Form

Question 3:

**Skipped**

You have multiple standalone AWS accounts and you want to decrease your AWS monthly charges. What should you do?

* 

Enable AWS tiered-pricing before provisioning resources

* 

Track the AWS charges that are incurred by the member accounts

* 

Add the accounts to an AWS Organization and use Consolidated Billing

**(Correct)**

* 

Try to remove unnecessary AWS accounts

**Explanation**

 Consolidated billing has the following benefits:

1- One bill – You get one bill for multiple accounts.

2- Easy tracking – You can track each account's charges, and download the cost data in .csv format.

3- Combined usage – If you have multiple standalone accounts, your charges might decrease if you add the accounts to an organization. AWS combines usage from all accounts in the organization to qualify you for volume pricing discounts.

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

***The other options are incorrect:***

***"Try to remove unnecessary AWS accounts" is incorrect.***Removing accounts or resources depends on your needs.

***"Track the AWS charges that are incurred by the member accounts" is incorrect.***Tracking the AWS charges will not decrease your charges.

***"Enable AWS tiered-pricing before provisioning resources" is incorrect.*** AWS tiered-pricing is applied for every AWS account regardless of whether it is part of an organization or not. With AWS, you can get volume-based discounts and realize important savings as your usage increases. For services such as S3 and data transfer OUT from EC2, pricing is tiered, meaning the more you use, the less you pay per GB. But if you have multiple AWS accounts, you can achieve even more discounts by adding them to an Organization and enable consolidated billing (because in that case, AWS will treat all the accounts as one account).

**References:**

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

<https://aws.amazon.com/pricing/>

Bottom of Form

Top of Form

Question 4:

**Skipped**

Which AWS service provides the EASIEST way to set up and manage a secure, well-architected, multi-account AWS environment?

* 

Amazon Macie

* 

AWS Systems Manager Patch Manager

* 

AWS Security Hub

* 

AWS Control Tower

**(Correct)**

**Explanation**

   You can use AWS Control Tower or AWS Organizations to set up and manage a secure, well-architected, multi-account AWS environment. With AWS Organizations, you build your environment from the ground up, which requires more upfront effort with full control over every aspect of your environment. AWS Control Tower provides built-in best-practice blueprints, guardrails, and automation features that help you build your multi-account environment quickly and easily.

   If you're a customer with multiple AWS accounts and teams, cloud setup and governance can be complex and time-consuming, slowing down the very innovation you're trying to speed up. AWS Control Tower provides the easiest way to set up a secure, multi-account AWS environment. For ongoing governance, you can enable pre-configured guardrails, which are clearly defined rules for security, operations, and compliance. Guardrails help prevent deployment of resources that don't conform to policies and continuously monitor deployed resources for nonconformance. The AWS Control Tower dashboard provides centralized visibility into the multi-account AWS environment, including accounts provisioned, guardrails enabled, and the compliance status of accounts.

Q: What is the difference between AWS Control Tower and AWS Organizations?

AWS Control Tower creates an abstraction or orchestration layer that combines and integrates the capabilities of several other AWS services, including AWS Organizations, AWS Single Sign-on, and AWS Service Catalog. AWS Control Tower offers an abstracted, automated, and prescriptive experience on top of AWS Organizations. It automatically sets up AWS Organizations as the underlying AWS service to organize accounts and implements preventive guardrails using service control policies (SCPs).

***The other options are incorrect:***

***“AWS Security Hub” is incorrect.*** AWS Security Hub aggregates, organizes, and prioritizes security alerts and findings from multiple AWS security services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, and supported third-party partners to help you analyze your security trends and identify the highest priority security issues.

**“AWS Systems Manager Patch Manager” is incorrect.**AWS Systems Manager helps you select and deploy operating system and software patches automatically across large groups of Amazon EC2 or on-premises instances. Through patch baselines, you can set rules to auto-approve select categories of patches to be installed, such as operating system or high severity patches. Systems Manager helps ensure that your software is up-to-date and meets your compliance policies.

***"Amazon Macie" is incorrect.***Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.

**References:**

<https://aws.amazon.com/controltower/>

Bottom of Form

Top of Form

Question 5:

**Skipped**

What is the Amazon ElastiCache service used for? (Choose TWO)

* 

Provide an in-memory data storage service

**(Correct)**

* 

Provide a Chef-compatible cache to speed up application response

* 

Distribute requests to multiple instances

* 

Stream desktop applications from the cloud to user devices

* 

Improve web application performance

**(Correct)**

**Explanation**

        Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory data store, instead of relying entirely on slower disk-based databases. Querying a database is always slower and more expensive than locating a copy of that data in a cache. By caching (storing) common database query results, you can quickly retrieve the data multiple times without having to re-execute the query.

***The other options are incorrect:***

***"Stream desktop applications from the cloud to user devices" is incorrect.***Amazon ElastiCache does not stream desktop applications from the cloud to end-user devices. The name of the service that performs this function is Amazon AppStream 2.0. AppStream 2.0 helps you move your existing desktop applications to AWS so that users can access them from anywhere.

**Interactively streaming your application from the cloud provides several benefits:**

1- Instant-on: Streaming your application with Amazon AppStream 2.0 lets your users start using your application immediately, without the delays associated with large file downloads and time-consuming installations.

2- Remove device constraints: You can leverage the compute power of AWS to deliver experiences that wouldn’t normally be possible due to the GPU, CPU, memory, or physical storage constraints of local devices.

3- Multi-platform support:You can take your existing applications and start streaming them to a computer without any modifications.

4- Easy updates: Because your application is centrally managed by Amazon AppStream 2.0, updating your application is as simple as providing a new version of your application to Amazon AppStream 2.0.

***"Distribute requests to multiple instances" is incorrect.*** Elastic Load Balancing is the service that can be used to distribute requests to multiple instances.

***"Provide a Chef-compatible cache to speed up application response" is incorrect.*** ElastiCache is not “Chef-compatible”. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. The AWS service that uses Chef and Puppet is AWS OpsWorks.

**References:**

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

Bottom of Form

Top of Form

Question 6:

**Skipped**

Which database service should you use if your application and data schema require "joins" or complex transactions?

* 

Amazon DocumentDB

* 

Amazon RDS

**(Correct)**

* 

Amazon DynamoDB

* 

AWS Outposts

**Explanation**

             If your database’s schema cannot be denormalized, and your application requires joins or complex transactions, consider using a relational database such as Amazon RDS.

***The other options are incorrect:***

***"Amazon DynamoDB" is incorrect.*** A NoSQL database such as Amazon DynamoDB is a type of non-relational database that uses a simple key-value method to store and retrieve data. DynamoDB does not support complex relational queries such as joins or complex transactions.

***"Amazon DocumentDB" is incorrect.***Document databases such as Amazon DocumentDB are designed to store semi-structured data as documents. Document databases do not support complex relational queries such as joins or complex transactions.

***"AWS Outposts" is incorrect.***AWS Outposts is an AWS service that delivers the same AWS infrastructure, native AWS services, APIs, and tools to virtually any customer on premises facility. With AWS Outposts, customers can run AWS services locally on their Outpost, including EC2, EBS, ECS, EKS, and RDS, and also have full access to services available in the Region. Customers can use AWS Outposts to securely store and process data that needs to remain on premises or in countries where there is no AWS region. AWS Outposts is ideal for applications that have low latency or local data processing requirements, such as financial services, healthcare, etc.

**References:**

<https://aws.amazon.com/products/databases/>

<https://aws.amazon.com/rds/>

Bottom of Form

Top of Form

Question 7:

**Skipped**

Which of the following services is an AWS repository management system that allows for storing, versioning, and managing your application code?

* 

AWS CodeCommit

**(Correct)**

* 

Amazon CodeGuru

* 

AWS CodePipeline

* 

AWS X-Ray

**Explanation**

            AWS CodeCommit is designed for software developers who need a secure, reliable, and scalable source control system to store and version their code. In addition, AWS CodeCommit can be used by anyone looking for an easy to use, fully managed data store that is version controlled. For example, IT administrators can use AWS CodeCommit to store their scripts and configurations. Web designers can use AWS CodeCommit to store HTML pages and images.

            AWS CodeCommit makes it easy for companies to host secure and highly available private Git repositories. Customers can use AWS CodeCommit to securely store anything from source code to binaries.

***The other options are incorrect:***

***AWS CodePipeline is incorrect.*** AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates.

***AWS X-Ray is incorrect.*** AWS X-Ray is a service that collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization.

***Amazon CodeGuru is incorrect.***Amazon CodeGuru is a developer tool that provides intelligent recommendations to improve code quality and identifying an application’s most expensive lines of code.

**References:**

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>         page 26

Bottom of Form

Top of Form

Question 8:

**Skipped**

Which of the following actions may reduce Amazon EBS costs? (Choose TWO)

* 

Distributing requests to multiple volumes

* 

Deleting unused Bucket ACLs

* 

Using reservations

* 

Deleting unnecessary snapshots

**(Correct)**

* 

Changing the type of the volume

**(Correct)**

**Explanation**

           With Amazon EBS, it is important to keep in mind that you are paying for provisioned capacity and performance, even if the volume is unattached or has very low write activity. To optimize storage performance and costs for Amazon EBS, monitor volumes periodically to identify unattached, underutilized or overutilized volumes, and adjust provisioning to match actual usage.

When you want to reduce the costs of Amazon EBS consider the following:

1- Delete Unattached Amazon EBS Volumes:

An easy way to reduce wasted spend is to find and delete unattached volumes. However, when EC2 instances are stopped or terminated, attached EBS volumes are not automatically deleted and will continue to accrue charges since they are still operating.

2- Resize or Change the EBS Volume Type:

Another way to optimize storage costs is to identify volumes that are underutilized and downsize them or change the volume type.

3- Delete Stale Amazon EBS Snapshots:

If you have a backup policy that takes EBS volume snapshots daily or weekly, you will quickly accumulate snapshots. Check for stale snapshots that are over 30 days old and delete them to reduce storage costs.

***The other options are incorrect:***

***"Deleting unused Bucket ACLs" is incorrect.***Amazon EBS does not use buckets. Buckets are used in S3 storage. Amazon S3 Bucket ACLs enable you to manage access to buckets. Each bucket has an ACL attached to it as a subresource. **You can use Bucket** **ACLs to grant basic read/write permissions to other AWS accounts**.

Note: [You have three options to control access to an Amazon S3 Bucket](https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s3-resources/):

1- IAM Policies

2- Bucket Policies

3- Bucket ACLs

***"Distributing requests to multiple volumes" is incorrect.***Amazon EBS is a storage service, not a compute service.

***"Using reservations" is incorrect.*** There are no reservations in Amazon EBS independent of Amazon EC2.

**References:**

<https://docs.aws.amazon.com/aws-technical-content/latest/cost-optimization-storage-optimization/optimizing-amazon-ebs-storage.html>

Bottom of Form

Top of Form

Question 9:

**Skipped**

You are planning to launch an advertising campaign over the coming weekend to promote a new digital product. It is expected that there will be heavy spikes in load during the campaign period, and you can’t afford any downtime. You need additional compute resources to handle the additional load. What is the most cost-effective EC2 instance purchasing option for this job?

* 

Savings Plans

* 

Reserved Instances

* 

Spot Instances

* 

On-Demand Instances

**(Correct)**

**Explanation**

             On Demand instances would help provision any extra capacity that the application may need without any interruptions.

***The other options are incorrect:***

***"Spot Instances" is incorrect.***Spot instances may be more cost effective, but AWS does not guarantee the availability of the instances. Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks.

***"Savings Plans" is incorrect.*** Using Savings Plans requires a contract of at least one year. Savings Plans is a flexible pricing model that offers low prices on EC2, Lambda, and Fargate usage, in exchange for a commitment to a consistent amount of compute usage (measured in $/hour) for a one or three-year term.

***"Reserved Instances" is incorrect.*** Using Reserved instances requires a contract of at least one year. Amazon EC2 Reserved Instances provide a significant discount (up to 75%) compared to On-Demand pricing. Reserved instances can be purchased for a one or three-year term so you are committing to pay for them throughout this time period even if you don't use them.

**References:**

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

Bottom of Form

Top of Form

Question 10:

**Skipped**

Which of the following resources can an AWS customer use to learn more about prohibited uses of the services offered by AWS?

* 

AWS Acceptable Use Policy

**(Correct)**

* 

AWS Service Control Policies (SCPs)

* 

AWS Budgets

* 

AWS Artifact

**Explanation**

            The AWS Acceptable Use Policy describes prohibited uses of the web services offered by AWS. For example, any activities that are illegal, that violate the rights of others, or that may be harmful to others are prohibited. If a customer violates the policy or authorizes or helps others to do so, AWS may suspend or terminate their use of the services.

***The other options are incorrect:***

***"AWS Artifact" is incorrect.***AWS Artifact provides on-demand access to AWS’ security and compliance reports. Examples of these reports include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports.

***"AWS Service Control Policies (SCPs)"*** ***is incorrect.*** AWS Service Control Policies (SCPs) or AWS Organizations Policies are a type of organization policy that you can use to manage permissions for all accounts in your organization. SCPs offer central control over the maximum available permissions for all member accounts in your organization. SCPs help you to ensure member accounts stay within your organization's access control guidelines. In SCPs, you can restrict which AWS services, resources, and individual API actions the users and roles in each member account can access.

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

**References:**

<https://aws.amazon.com/aup/>

Bottom of Form

Top of Form

Question 11:

**Skipped**

You have just finished writing your application code. Which service can be used to automate the deployment and scaling of your application?

* 

Amazon Simple Storage Service

* 

AWS CodeCommit

* 

Amazon CodeGuru

* 

AWS Elastic Beanstalk

**(Correct)**

**Explanation**

        AWS Elastic Beanstalk is considered a Platform as a Service (PaaS). It is an easy-to-use service for deploying, scaling and updating web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

***The other options are incorrect:***

***"Amazon Simple Storage Service" is incorrect.***Amazon Simple Storage Service (S3) is a storage service.

***"Amazon CodeGuru" is incorrect.*** Amazon CodeGuru is a developer tool that provides intelligent recommendations to improve code quality and identifying an application’s most expensive lines of code.

***"AWS CodeCommit" is incorrect.*** AWS CodeCommit is a source code control service that hosts secure Git-based code repositories. AWS CodeCommit is designed for software developers who need a secure, reliable, and scalable source control system to store and version their code.

**References:**

<https://aws.amazon.com/elasticbeanstalk/>

Bottom of Form

Top of Form

Question 12:

**Skipped**

What does Amazon GuardDuty do to protect AWS accounts and workloads?

* 

Continuously monitors AWS infrastructure and helps detect threats such as attacker reconnaissance or account compromise

**(Correct)**

* 

Notifies AWS customers about abuse events once they are reported

* 

Checks security groups for rules that allow unrestricted access to AWS resources

* 

Helps AWS customers identify the root cause of potential security issues

**Explanation**

      Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

      With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in the AWS Cloud. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats.

      Amazon GuardDuty provides broad protection of your AWS accounts, workloads, and data by helping to identify threats such as attacker reconnaissance, instance compromise, and account compromise.

***The other options are incorrect:***

***" Helps AWS customers identify the root cause of potential security issues" is incorrect.*** Amazon Detective is the service that helps AWS customers analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities.

How does Amazon Detective differ from Amazon GuardDuty?

     Amazon GuardDuty is helpful in alerting you when something is wrong and pointing out where to go to fix it. But sometimes, there might be a security finding where you need to dig a lot deeper and analyze more information to isolate the root cause and take action.

     Amazon Detective simplifies this process by enabling you to easily investigate and quickly get to the root cause of a security finding. Amazon Detective analyzes trillions of events from multiple data sources such as Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail logs, and automatically creates a unified view of user and resource interactions over time, with all the context and details in one place to help you quickly analyze and get to the root cause of a security finding.

     For example, an Amazon GuardDuty finding, like an unusual Console Login API call, can be quickly investigated in Amazon Detective with details about the API call trends over time, and user login attempts on a geolocation map. These details enable you to quickly identify if you think it is legitimate or an indication of a compromised AWS resource.

***“Checks security groups for rules that allow unrestricted access to AWS resources” is incorrect.***Security Groups Check is one of the core security checks provided by AWS Trusted Advisor. AWS Trusted Advisor continuously checks security groups for rules that allow unrestricted access to AWS resources. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

***“Notifies AWS customers about abuse events once they are reported” is incorrect.***AWS Personal Health Dashboard is the service that notifies AWS customers about abuse events once they are reported. AWS addresses many different types of potentially abusive activity such as phishing, malware, spam, and denial of service (DoS)/ distributed denial of service (DDoS) incidents. When abuse is reported, AWS alerts customers so they can take the necessary remediation action. AWS Personal Health Dashboard can also help customers build automation for handling abuse events and the actions to remediate them.

When customers receive abuse notifications via email only, it is challenging to manage the alerts because emails could be lost or could be sent to incorrect contacts on the account, or they might not be reviewed in a timely manner. AWS addressed those challenges by surfacing abuse alerts in the AWS Personal Health Dashboard (PHD) where customers are already monitoring the health of their AWS environments.

**References:**

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

<https://aws.amazon.com/blogs/mt/automating-processes-for-handling-and-remediating-aws-abuse-alerts/>

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

Bottom of Form

Top of Form

Question 13:

**Skipped**

Which of the following procedures can reduce latency when your end users are retrieving data? (Choose TWO)

* 

Replicate media assets to at least two availability zones

* 

Store media assets in the region closest to your end users

**(Correct)**

* 

Store media assets on an additional EBS volume and increase the capacity of your server

* 

Reduce the size of media assets using the Amazon Elastic Transcoder

* 

Store media assets in S3 and use CloudFront to distribute these assets

**(Correct)**

**Explanation**

             Amazon CloudFront is a fast Content Delivery Network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

CloudFront is the best solution to reduce latency if you have users from different places around the world.

             Storing media assets in a region closer to the end-users can help reduce latency for those users. This is because these assets will travel a shorter distance over the network.

***The other options are incorrect:***

***"Store media assets on an additional EBS volume and increase the capacity of your server" is incorrect.***Storing media assets on an additional EBS volume or increasing the capacity of your server does nothing with regards to latency. The question does not mention that you are facing heavy workloads, so increasing the capacity of your EC2 instances to more powerful types will be a waste of money in this scenario.

***"Replicate media assets to at least two availability zones" is incorrect.***Replicating your media assets on at least two availability zones may improve the availability of your application but will not reduce latency especially if these AZs exist in the same region.

***"Reduce the size of media assets using the Amazon Elastic Transcoder" is incorrect.*** Amazon Elastic Transcoder lets you convert (or “transcode”) media files from their source format into versions that will playback on mobile devices, tablets, web browsers, and connected televisions.

**References:**

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

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html>

Bottom of Form

Top of Form

Question 14:

**Skipped**

What are the main differences between an IAM user and an IAM role in AWS? (Choose TWO)

* 

An IAM user has permanent credentials associated with it, however a role has temporary credentials associated with it

**(Correct)**

* 

IAM users are more cost effective than IAM roles

* 

An IAM user is uniquely associated with only one person, however a role is intended to be assumable by anyone who needs it

**(Correct)**

* 

An IAM user has temporary credentials associated with it, however a role has permanent credentials associated with it

* 

A role is uniquely associated with only one person, however an IAM user is intended to be assumable by anyone who needs it

**Explanation**

              An IAM role is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it (as long as they are authorized to do so). Also, a role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user.

***The other options are incorrect:***

***"A role is uniquely associated with only one person, however an IAM user is intended to be assumable by anyone who needs it" is incorrect.***An IAM user is uniquely associated with only **one person**, however a role is intended to be assumable by **anyone** who is authorized to use it.

***"An IAM user has temporary credentials associated with it, however a role has permanent credentials associated with it" is incorrect.***An IAM user has **permanent** credentials associated with it, however a role has **temporary** credentials associated with it.

***"IAM users are more cost effective than IAM roles" is incorrect.***AWSIAM and its features are offered at no additional charge.

**References:**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html>

Bottom of Form

Top of Form

Question 15:

**Skipped**

Who is responsible for scaling a DynamoDB database in the AWS Shared Responsibility Model?

* 

Your development team

* 

AWS

**(Correct)**

* 

Your security team

* 

Your internal DevOps team

**Explanation**

          DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB enables customers to offload the administrative burdens of operating and scaling distributed databases to AWS so that they do not have to worry about hardware provisioning, setup and configuration, throughput capacity planning, replication, software patching, or cluster scaling.

**References:**

<https://aws.amazon.com/dynamodb/faqs/>

Bottom of Form

Top of Form

Question 16:

**Skipped**

What does the AWS "Business" support plan provide? (Choose TWO)

* 

Proactive Technical Account Management

* 

Less than 15 minutes response-time support if your business critical system goes down

* 

Consultative review and guidance based on your applications

* 

Access to the full set of Trusted Advisor checks

**(Correct)**

* 

AWS Support API

**(Correct)**

**Explanation**

       AWS recommend Business Support if you have production workloads on AWS and want 24x7 access to technical support and architectural guidance in the context of your specific use-cases.

**In addition to what is available with Basic Support, Business Support provides:**

**1- AWS Trusted Advisor** - Access to the full set of Trusted Advisor checks and guidance to provision your resources following best practices to help reduce costs, increase performance and fault tolerance, and improve security.

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

**3- Enhanced Technical Support** – 24x7 access to Cloud Support Engineers via phone, chat, and email. You can have an unlimited number of contacts that can open an unlimited amount of cases.

Response times are as follows:

- General Guidance - < 24 hours

- System Impaired - < 12 hours

- Production System Impaired - < 4 hours

- Production System Down - < 1 hour

**4- Architecture Support – Contextual guidance** on how services fit together to meet your specific use-case, workload, or application.

**5- AWS Support API**- Programmatic access to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status.

**6- Access to Proactive Support Programs**– Ability to purchase Infrastructure Event Management for an additional fee. This provides Architecture and scaling guidance, and real-time operational support during the preparation and execution of planned events, product launches, and migrations.

***The other options are incorrect:***

***"Consultative review and guidance based on your applications" is incorrect.*** [AWS support plans](https://aws.amazon.com/premiumsupport/plans/) differ on what level of architectural support each of them provides. The AWS support plan that provides **consultative review** **and guidance** based on your applications is AWS **Enterprise** support.

The AWS **Business** Support provides **contextual architectural guidance**on what AWS products, features, and services to use to best support your specific use-case, workload, or application.

The AWS **Developer** Support provides **general architectural guidance** on how to use AWS products, features, and services together to best support your specific use-case, workload, or application.

***"Less than 15 minutes response-time support if your business critical system goes down" is incorrect.***The AWS Business support plan provide 1-hour response time support if your production system goes down. If you want less than 15-minutes response time, you must subscribe to the AWS Enterprise support plan.

***"Proactive Technical Account Management" is incorrect.***Proactive Technical Account Managementis only available for the AWS Enterprise support plan. A Technical Account Manager (TAM) is your designated technical point of contact who provides advocacy and guidance to help plan and build solutions using best practices, coordinate access to subject matter experts and product teams, and proactively keep your AWS environment operationally healthy.

**References:**

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

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

<https://aws.amazon.com/premiumsupport/plans/business/>

Bottom of Form

Top of Form

Question 17:

**Skipped**

Which of the following Cloud Computing deployment models eliminates the need to run and maintain physical data centers?

* 

Cloud

**(Correct)**

* 

On-premises

* 

PaaS

* 

IaaS

**Explanation**

**There are three Cloud Computing Deployment Models:**

**1- Cloud:**

        A cloud-based application is fully deployed in the cloud and all parts of the application run in the cloud. This Cloud Computing deployment model eliminates the need to run and maintain physical data centers.

**2- Hybrid:**

       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 (On-premises data centers).

**3- On-premises:**

       Deploying resources on-premises, using virtualization and resource management tools, is sometimes called “private cloud”. On-premises deployment does not provide many of the benefits of cloud computing but is sometimes sought for its ability to provide dedicated resources.

***The other options are incorrect:***

Iaas, PaaS, and SaaS are not deployment models. They represent the different use cases of Cloud Computing, and the different levels of control customers need over their IT resources.

***IaaS is incorrect.***Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.

***PaaS is incorrect.***Platform as a Service (PaaS) removes the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as 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.

***SaaS -***Software as a Service (SaaS) provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not 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 piece software. A common example of a SaaS application is the web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

**References:**

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

Bottom of Form

Top of Form

Question 18:

**Skipped**

What are the benefits of the AWS Organizations service? (Choose TWO)

* 

Help organizations design and maintain an accelerated path to successful cloud adoption

* 

Manage your organization’s payment methods

* 

Control access to AWS services

**(Correct)**

* 

Consolidate billing across multiple AWS accounts

**(Correct)**

* 

Help organizations achieve their desired business outcomes with AWS

**Explanation**

       AWS Organizations has five main benefits:

1) Centrally manage access polices across multiple AWS accounts.

2) Automate AWS account creation and management.

3) Control access to AWS services.

4) Consolidate billing across multiple AWS accounts.

5) Configure AWS services across multiple accounts.

\*\* Control access to AWS services: AWS Organizations allows you to restrict what services and actions are allowed in your accounts. You can use **Service Control Policies (SCPs)** to apply permission guardrails on AWS Identity and Access Management (IAM) users and roles. For example, you can apply an **SCP** that restricts users in accounts in your organization from launching any resources in regions that you do not explicitly allow.

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

***The other options are incorrect:***

***"Help organizations achieve their desired business outcomes with AWS" is incorrect.***AWS Professional Services is the service that helps organizations achieve their desired business outcomes with AWS.

***"Manage your organization’s payment methods" is incorrect.*** AWS Billing and Cost Management is the service that allows you to manage your organization’s payment methods.

***"Help organizations design and maintain an accelerated path to successful cloud adoption" is incorrect.***AWS Professional Services is the service that helps organizations design and travel an accelerated path to successful cloud adoption

**References:**

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

Bottom of Form

Top of Form

Question 19:

**Skipped**

Which of the following AWS support plans provides access to only the core AWS Trusted Advisor checks?

* 

Developer & Business Support

* 

Business & Enterprise Support

* 

Developer & Enterprise Support

* 

Basic & Developer Support

**(Correct)**

**Explanation**

      AWS Trusted Advisor offers a rich set of best practice checks and recommendations across five categories: cost optimization, security, fault tolerance, performance, and service limits. AWS **Basic** Support and AWS **Developer** Support customers get access to **6** **core security checks**(S3 Bucket Permissions, Security Groups - Specific Ports Unrestricted, IAM Use, MFA on Root Account, EBS Public Snapshots, RDS Public Snapshots) and **50 service limit checks.**

      AWS **Business** Support and AWS **Enterprise** Support customers get access to **ALL** 115 Trusted Advisor checks (14 cost optimization, 17 security, 24 fault tolerance, 10 performance, and 50 service limits).

**References:**

<https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html>

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

Bottom of Form

Top of Form

Question 20:

**Skipped**

You are working as a web app developer. You are currently facing issues in media playback for mobile devices because your media format is not supported. Which of the following AWS services can help you convert your media into another format?

* 

Amazon S3

* 

Amazon Rekognition

* 

Amazon Elastic Transcoder

**(Correct)**

* 

Amazon Pinpoint

**Explanation**

              Amazon Elastic Transcoder is a media transcoding service. It is designed to be a highly scalable, easy-to-use, and cost-effective way to convert (or transcode) media files from their source format into versions that will play back on devices like smartphones, tablets, and PCs.

***The other options are incorrect:***

***Amazon Pinpoint is incorrect.***Amazon Pinpoint is used by marketers to engage their customers by sending targeted email, SMS, push notifications, and voice messages.

***Amazon Rekognition is incorrect.*** Amazon Rekognition allows you to add image and video analysis to your applications. For example, you can use it detect faces in millions of images uploaded to S3.

***Amazon S3 is incorrect.*** Amazon S3 is a storage service.

**References:**

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>   page 44

Bottom of Form

Top of Form

Question 21:

**Skipped**

How can you increase your application’s fault-tolerance while it is being hosted in AWS?

* 

Deploy your application across multiple EC2 instances

* 

Deploy your application across multiple Availability Zones

**(Correct)**

* 

Host your application on one powerful EC2 instance type instead of multiple smaller instances

* 

Deploy the underlying application resources across multiple subnets

**Explanation**

          The fault tolerance of an application is its ability to recover gracefully from failures. Deploying the application resources across multiple availability zones will guarantee that even if one availability zone goes down, there will still be other availability zones to run the application efficiently.

***The other options are incorrect:***

***"Deploy your application across multiple*** ***EC2 instances" is incorrect.***

This option is incorrect for two reasons:

1) It is not mentioned whether those instances will run in a single Availability Zone or multiple Availability Zones.

2) Deploying your application across multiple EC2 instances is costly and may not be necessary. The better alternative is to configure EC2 Auto Scaling to automatically add or remove instances and run the **required** number of instances **only**.

***"Deploy the underlying application resources across multiple subnets" is incorrect.***You can have multiple subnets in the same availability zone, so to ensure fault tolerance you must deploy into multiple subnets in multiple availability zones.

***"Host your application on one powerful EC2 instance type instead of multiple smaller instances" is incorrect.***Hosting your application on one powerful instance is not a best practice, because as soon as that instance fails, the entire application will fail. For that reason, you should deploy your application across multiple instances in multiple availability zones to increase your application’s fault-tolerance.

**References:**

<https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/global-infrastructure.html>

Bottom of Form

Top of Form

Question 22:

**Skipped**

A company is migrating production workloads to AWS, and they are concerned about cost management across different departments. Which option should the company implement to categorize and track AWS spending?

* 

Use Amazon Aurora to forecast AWS spending based on usage

* 

Apply cost allocation tags to segment AWS costs by different projects and departments

**(Correct)**

* 

Configure AWS Price List API to receive billing updates for each department automatically

* 

Use the AWS Pricing Calculator service to monitor the costs incurred by each department

**Explanation**

     A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. A key can have more than one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track AWS costs across different departments.

***The other options are incorrect:***

***"Use Amazon Aurora to forecast AWS spending based on usage" is incorrect.***Amazon Aurora is a relational database service, not a cost management service. The name of the service that performs this function is AWS Cost Explorer.

Additional information:

AWS Cost Explorer is a free tool that you can use to view your costs and usage. You can view data up to the last 13 months, forecast how much you are likely to spend for the next twelve months. You can use AWS Cost Explorer to see patterns in how much you spend on AWS resources over time, identify areas that need further inquiry, and see trends that you can use to understand your costs. AWS Cost Explorer allows you to 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 a number of filtering dimensions (e.g., AWS Service, Region, Linked Account, etc.)

***"Configure AWS Price List API to receive billing updates for each department automatically" is incorrect.***AWS Price List API is used to know the prices of AWS services. AWS Price List API does not send billing updates to AWS Customers.

***"Use the AWS Pricing Calculator service to monitor the costs incurred by each department" is incorrect.***AWS Pricing Calculator does not record any information about your AWS cost and usage. AWS Pricing Calculator is just a tool for estimating your monthly AWS bill based on your expected usage. For example, to estimate your monthly AWS CloudFront bill, you just enter your expected CloudFront usage (Data Transfer Out, Number of requests, etc.) and AWS Pricing Calculator provides an estimate of your monthly bill for CloudFront.

**References:**

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

Bottom of Form

Top of Form

Question 23:

**Skipped**

You have been tasked with auditing the security of your VPC. As part of this process, you need to start by analyzing what inbound and outbound traffic is allowed on your EC2 instances.What two parts of the VPC do you need to check to accomplish this task?

* 

Network ACLs and Traffic Manager

* 

Security Groups and Network ACLs

**(Correct)**

* 

Security Groups and Internet Gateways

* 

Network ACLs and Subnets

**Explanation**

           Security Groups and Network Access Control Lists (Network ACLs) are the two parts of the VPC Security Layer. Security Groups are a firewall at the instance layer, and Network ACLs are a firewall at the subnet layer.

***The other options are incorrect:***

***"Network ACLs and Traffic Manager" is incorrect.*** Traffic manager is an Azure service not AWS service.

***"Security Groups and Internet Gateways" is incorrect.***Internet Gateways provide access for a VPC and subnet to reach the internet. They are not directly attached to EC2 instances.

***"Network ACLs*** ***and Subnets" is incorrect.*** Subnets are where EC2 instances reside, but they do not actually control ingress and egress traffic themselves.

**References:**

<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html>

Bottom of Form

Top of Form

Question 24:

**Skipped**

Which feature enables users to sign into their AWS accounts with their existing corporate credentials?

* 

WAF rules

* 

Federation

**(Correct)**

* 

Access keys

* 

IAM Permissions

**Explanation**

        With Federation, you can use single sign-on (SSO) to access your AWS accounts using credentials from your corporate directory. Federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML), to exchange identity and security information between an identity provider (IdP) and an application.

**AWS offers multiple options for federating your identities in AWS:**

**1- AWS Identity and Access Management (IAM):** You can use AWS Identity and Access Management (IAM) to enable users to sign in to their AWS accounts with their existing corporate credentials.

**2- AWS Directory Service:**AWS Directory Service for Microsoft Active Directory, also known as AWS Microsoft AD, uses secure Windows trusts to enable users to sign in to the AWS Management Console, AWS Command Line Interface (CLI), and Windows applications running on AWS using their existing corporate Microsoft Active Directory credentials.

**3- AWS Single-Sign-On (AWS SSO) Service:**You can use the AWS SSO service to federate your identities into your AWS environment.

***The other options are incorrect:***

***"WAF rules" is incorrect.***AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that block malicious traffic.

You use WAF rules in a web ACL to block web requests based on criteria like the following:

- Scripts that are likely to be malicious. Attackers embed scripts that can exploit vulnerabilities in web applications. This is known as cross-site scripting (XSS).

- Malicious requests from a set of IP addresses or address ranges.

- SQL code that is likely to be malicious. Attackers try to extract data from your database by embedding malicious SQL code in a web request. This is known as SQL injection.

***"IAM Permissions" is incorrect.*** IAM Permissions let you specify the desired access to AWS resources. Permissions are granted to IAM entities (users, groups, and roles) and by default these entities start with no permissions. In other words, IAM entities can do nothing in AWS until you grant them your desired permissions.

***"Access keys" is incorrect.*** Access keys are long-term credentials for an AWS IAM user or the AWS account root user. Access keys are not used for signing in to your account. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

**References:**

<https://aws.amazon.com/identity/federation/>

Bottom of Form

Top of Form

Question 25:

**Skipped**

What is the maximum amount of data that can be stored in S3 in a single AWS account?

* 

100 PetaBytes

* 

10 Exabytes

* 

5 TeraBytes

* 

Virtually unlimited storage

**(Correct)**

**Explanation**

             The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes.

**References:**

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html>

Bottom of Form

Top of Form

Question 26:

**Skipped**

Which statement is true regarding AWS pricing? (Choose TWO)

* 

There are no reservations on AWS, you only pay for what you use

* 

You only pay for the individual services that you need with no long-term contracts

**(Correct)**

* 

You have no responsibility for third-party software license costs

* 

With the AWS pay-as-you-go pricing model, you do not have to pay any upfront fee

**(Correct)**

* 

For some services, you have to pay a startup fee in order to get the service running

**Explanation**

AWS provides three pricing models:

1- Pay-as-you-go

2- Save when you reserve

3- Pay less by using more

          With the AWS pay-as-you-go model, you only pay for what you consume, you do not have to pay any money upfront and there are no long term contracts. The AWS pay-as-you-go pricing is similar to how you pay for utilities like water and electricity. You only pay for the services you consume, and once you stop using them, there are no additional costs or termination fees.

**The other options are incorrect:**

***"For some services, you have to pay a startup fee in order to get the service running" is incorrect.*** There are no startup fees for any AWS service.

***"There are no reservations on AWS, you only pay for what you use" is incorrect.***You have the choice to reserve capacity on AWS. If you are committed to use a service for a long time, then it is better to reserve to get discounts. For example Amazon EC2 Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing.

***"You have no responsibility for third-party software license costs" is incorrect.*** You are responsible for buying a license for any third-party software you install on AWS. You can buy a license directly from the software vendor - or buy it from the AWS Marketplace and benefit from the flexible, pay-as-you-go pricing options.

**References:**

<https://aws.amazon.com/pricing/>

Bottom of Form

Top of Form

Question 27:

**Skipped**

Which of the following requires an access key ID and a secret access key to get long-lived programmatic access to AWS resources? (Choose TWO)

* 

IAM user

**(Correct)**

* 

IAM role

* 

AWS account root user

**(Correct)**

* 

TAM

* 

IAM group

**Explanation**

           An AWS IAM user might need to make API calls or use the AWS CLI. In that case, you need to create an access key (access key ID and a secret access key) for that user. You can create IAM user access keys with the IAM console, AWS CLI,or AWS API. To create access keys for your AWS account root user, you must use the AWS Management Console.

**Note:**Having access keys for your root user is not considered best practice. Anyone who has root user access keys for your AWS account has unrestricted access to all the resources in your account, including billing information. If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to.

The following tasks can only be performed if you have root user credentials:

1- Change your account settings. This includes the account name, root user password, and email address.

2- Activate IAM access to the Billing and Cost Management console.

3- Close your AWS account.

4- Change your AWS Support plan or Cancel your AWS Support plan.

5- Register as a seller in the Reserved Instance Marketplace.

6- Configure an Amazon S3 bucket to enable MFA (multi-factor authentication) Delete. The AWS account owner (root account) configure MFA delete on a bucket to help ensure that the data in their bucket cannot be accidentally deleted.

For a full list of the tasks that require root user credentials visit this link:

<https://docs.aws.amazon.com/general/latest/gr/root-vs-iam.html#aws_tasks-that-require-root>

***The other options are incorrect:***

***IAM group and IAM role are incorrect.*** An IAM group and an IAM role represent other IAM Identities that serve different purposes in the AWS IAM.

***TAM is incorrect.*** TAM refers to the AWS technical account manager.

**References:**

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

Bottom of Form

Top of Form

Question 28:

**Skipped**

What is the benefit of Amazon EBS volumes being automatically replicated within the same availability zone?

* 

Traceability

* 

Accessibility

* 

Elasticity

* 

Durability

**(Correct)**

**Explanation**

         Durability refers to the ability of a system to assure data is stored and data remains consistent in the system as long as it is not changed by legitimate access. This means that data should not become corrupted or disappear due to a system malfunction.

         Durability is used to measure the likelihood of data loss. For example, assume you have confidential data stored in your Laptop. If you make a copy of it and store it in a secure place, you have just improved the durability of that data. It is much less likely that all copies will be simultaneously destroyed.

        Amazon EBS volume data is replicated across multiple servers in an Availability Zone to prevent the loss of data from the failure of any single component. The replication of data makes EBS volumes 20 times more durable than typical commodity disk drives, which fail with an AFR (annual failure rate) of around 4%. For example, if you have 1,000 EBS volumes running for 1 year, you should expect 1 to 2 will have a failure.

Additional information:

      Amazon S3 is also considered a durable storage service. Amazon S3 is designed for 99.999999999% (11 9’s) durability. This means that if you store 100 billion objects in S3, you will lose one object at most.

***The other options are incorrect:***

***"Elasticity" is incorrect.*** Elasticity refers to the ability of a system to scale its resources up or down based on demand.

***"Traceability" is incorrect.***Traceability is related to the tracking of changes made throughout a system, and not related to replicating EBS data.

***"Accessibility" is incorrect.*** Replicating the volume does not impact how you can access it. You can access EBS volumes using EC2 after mounting them to the operating system.

**References:**

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

Bottom of Form

Top of Form

Question 29:

**Skipped**

Which of the following AWS Support Plans gives you 24/7 access to Cloud Support Engineers via email & phone? (Choose TWO)

* 

Developer

* 

Business

**(Correct)**

* 

Enterprise

**(Correct)**

* 

Standard

* 

Premium

**Explanation**

        For Technical Support, each of the Business and the Enterprise support plans provides 24x7 phone, email, and chat access to Support Engineers.

***The other options are incorrect:***

***"Premium" and "Standard "are incorrect.*** Premium and Standard are not valid support plans on AWS.

***"Developer" is incorrect.***This plan does not include phone support 24/7.

**References:**

<https://aws.amazon.com/premiumsupport/compare-plans/>

Bottom of Form

Top of Form

Question 30:

**Skipped**

The AWS account administrator of your company has been fired. With the permissions granted to him as an administrator, he was able to create multiple IAM user accounts and access keys. Additionally, you are not sure whether he has access to the AWS root account or not. What should you do immediately to protect your AWS infrastructure? (Choose TWO)

* 

Download all the attached policies in a safe place

* 

Rotate all access keys

**(Correct)**

* 

Use the CloudWatch service to check all API calls that have been made in your account since the administrator was fired

* 

Delete all IAM accounts and recreate them

* 

Change the email address and password of the root user account and enable MFA

**(Correct)**

**Explanation**

To protect your AWS infrastructure in this situation you should lock down your root user account and all IAM user accounts that the administrator had access to.

To protect your AWS infrastructure you should:

1- Change the email address and the password of the root user account

2- Enable MFA on the root user account

4- Rotate (change) all access keys for all accounts

3- Change the user name and password of all IAM users

5- Enable MFA on all IAM user accounts

***The other options are incorrect:***

***"Delete all IAM accounts and recreate them" is incorrect.*** Deleting all IAM accounts is not necessary, and it could cause  disruption to your operations.

***"Download all the attached policies in a safe place" is incorrect.*** IAM policies are used to authorize users to perform actions on AWS resources. Downloading them save you some time if they were deleted, but it is not an immediate first step to take to protect your AWS infrastructure.

***"Use the CloudWatch service to check all API calls that have been made in your account since the administrator was fired" is incorrect.***CloudTrail is the service that gives you a complete history of the API calls that have been made in your account from all users, not CloudWatch.

**References:**

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

Bottom of Form

Top of Form

Question 31:

**Skipped**

Which of the following factors affect Amazon CloudFront cost? (Choose TWO)

* 

Number of Volumes

* 

Storage Class

* 

Number of Requests

**(Correct)**

* 

Traffic Distribution

**(Correct)**

* 

Instance type

**Explanation**

     Amazon CloudFront charges are based on the data transfer out of AWS and requests used to deliver content to your customers. There are no upfront payments or fixed platform fees, no long-term commitments, no premiums for dynamic content, and no requirements for professional services to get started.

To estimate the costs of an Amazon CloudFront distribution consider the following:

- Traffic Distribution: Data transfer and request pricing varies across geographic regions, and pricing is based on the edge location through which your content is served.

- Requests: The number and type of requests (HTTP or HTTPS) made and the geographic region in which the requests are made.

- Data Transfer OUT: The amount of data transferred out of your Amazon CloudFront edge locations.

Note:Data Transfer IN is free. There is no charge forinbound data transferred from AWS services such as Amazon S3 or Elastic Load Balancing.

***The other options are incorrect:***

***"Number of Volumes" and "Storage Class" are incorrect.***CloudFront is a caching and Content Delivery Network (CDN) service, not a storage service. It does not have the concept of volumes or storage classes.

***"Instance type" is incorrect.*** Instance type is a factor that affects Amazon EC2 costs, not Amazon CloudFront costs.

**References:**

<https://aws.amazon.com/cloudfront/pricing/>

Bottom of Form

Top of Form

Question 32:

**Skipped**

​The elasticity of the AWS Cloud enables customers to save costs when compared to traditional hosting providers. What can AWS customers do to benefit from the elasticity of the AWS Cloud? (Choose TWO)

* 

Use Serverless Computing whenever possible

**(Correct)**

* 

Deploy your resources in another region

* 

Use Elastic Load Balancing

* 

Use Amazon EC2 Auto Scaling

**(Correct)**

* 

Deploy your resources across multiple Availability Zones

**Explanation**

              Another way you can save money with AWS is by taking advantage of the platform’s elasticity. Elasticity means the ability to scale up or down when needed. This concept is most closely associated with the AWS auto scaling which monitors your applications and automatically adjusts capacity (up or down) to maintain steady, predictable performance at the lowest possible cost.

              Serverless Computing provides the highest level of elasticity. Serverless enables you to build modern applications with increased agility and lower total cost of ownership. Serverless allows you to run applications and services without thinking about servers. It eliminates infrastructure management tasks such as server or cluster provisioning, patching, operating system maintenance, and capacity provisioning. With serverless computing, everything required to run and scale your application with high availability is handled for you.

***The other options are incorrect:***

***"Deploy your resources in another region" is incorrect.*** You may want to deploy your resources in another region to enable faster disaster recovery. Also, deploying your resources in multiple regions worldwide reduce latency to global users.

***"Use Elastic Load Balancing" is incorrect.*** Elastic Load Balancing does not scale resources. Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.

***"Deploy your resources across multiple Availability Zones" is incorrect.*** Deploying your resources across multiple Availability Zones helps you maintain high availability of your infrastructure.

**References:**

<https://wa.aws.amazon.com/wat.concept.elasticity.en.html>

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

Bottom of Form

Top of Form

Question 33:

**Skipped**

What are the benefits of the AWS Marketplace service? (Choose TWO)

* 

Per-second billing

* 

Provides cheaper options for purchasing Amazon EC2 on-demand instances

* 

Provides flexible pricing options that suit most customer needs

**(Correct)**

* 

Protects customers by performing periodic security checks on listed products

**(Correct)**

* 

Provides software solutions that run on AWS or any other Cloud vendor

**Explanation**

              The AWS Marketplace is a curated digital catalog that makes it easy for customers to find, buy, and immediately start using the software and services that customers need to build solutions and run their businesses. The AWS Marketplace includes thousands of software listings from popular categories such as security, networking, storage, machine learning, business intelligence, database, and DevOps. AWS Marketplace is designed for Independent Software Vendors (ISVs), Value-Added Resellers (VARs), and Systems Integrators (SIs) who have software products they want to offer to customers in the cloud. Partners use AWS Marketplace to be up and running in days and offer their software products to customers around the world.

The AWS Marketplace provides value to buyers in several ways:

1- It simplifies software licensing and procurement with flexible pricing options and multiple deployment methods. Flexible pricing options include free trial, hourly, monthly, annual, multi-year, and BYOL.

2- Customers can quickly launch pre-configured software with just a few clicks, and choose software solutions in AMI and SaaS formats, as well as other formats.

3- It ensures that products are scanned periodically for known vulnerabilities, malware, default passwords, and other security-related concerns.

***The other options are incorrect:***

***"Provides cheaper options for purchasing Amazon EC2 on-demand instances" is incorrect.***The AWS marketplace cannot be used to buy Amazon EC2 on-demand instances.

***"Provides software solutions that run on AWS or any other Cloud vendor" is incorrect.***The AWS Marketplace provides software solutions that run on AWS only.

***"Per-second billing" is incorrect.***The AWS marketplace pricing options include free trial, hourly, monthly, annual, multi-year, and BYOL. Per-second billing is found on AWS resources and services only. It is not found in the marketplace.

**References:**

<https://aws.amazon.com/marketplace>

<https://docs.aws.amazon.com/marketplace/latest/userguide/what-is-marketplace.html>

Bottom of Form

Top of Form

Question 34:

**Skipped**

Which of the following are part of the seven design principles for security in the cloud? (Choose TWO)

* 

Use IAM roles to grant temporary access instead of long-term credentials

**(Correct)**

* 

Use manual monitoring techniques to protect your AWS resources

* 

Enable real-time traceability

**(Correct)**

* 

Never store sensitive data in the cloud

* 

Scale horizontally to protect from failures

**Explanation**

There are seven design principles for security in the cloud:

1- Implement a strong identity foundation: Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize privilege management and reduce or even eliminate reliance on long-term credentials.

2- Enable traceability: Monitor, alert, and audit actions and changes to your environment in real time. Integrate logs and metrics with systems to automatically respond and take action.

3- Apply security at all layers: Rather than just focusing on protection of a single outer layer, apply a defense-in-depth approach with other security controls. Apply to all layers (e.g., edge network, VPC, subnet, load balancer, every instance, operating system, and application).

4- Automate security best practices: Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.

5- Protect data in transit and at rest: Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.

6- Keep people away from data: Create mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of loss or modification and human error when handling sensitive data.

7- Prepare for security events: Prepare for an incident by having an incident management process that aligns to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

***The other options are incorrect:***

***"Scale horizontally to protect from failures" is incorrect.*** Protecting from networking failures due to hardware issues or mis-configuration is not related to security. Protecting from failures and scaling horizontally are much more related to the reliability of your system.

***"Never store sensitive data in the cloud" is incorrect.*** AWS provides encryption and access control tools that allow you to easily encrypt your data in transit and at rest and help ensure that only authorized users can access it.

***"Use manual monitoring techniques to protect your AWS resources" is incorrect.***Automating security tasks on AWS enables you to be more secure. For example, you can automate infrastructure and application security checks to continually enforce your security and compliance controls and help ensure confidentiality, integrity, and availability at all times.

**References:**

<https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf>

Bottom of Form

Top of Form

Question 35:

**Skipped**

What are some of the benefits of using On-Demand EC2 instances? (Choose TWO)

* 

They remove the need to buy “safety net” capacity to handle periodic traffic spikes

**(Correct)**

* 

They only require 1-2 days for setup and configuration

* 

You can increase or decrease your compute capacity depending on the demands of your application

**(Correct)**

* 

They are cheaper than all other EC2 options

* 

They provide free capacity when testing your new applications

**Explanation**

       With On-Demand instances, you pay for compute capacity by the hour or the second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay for what you use. The use of On-Demand instances frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs. On-Demand instances also remove the need to buy “safety net” capacity to handle periodic traffic spikes.

***The other options are incorrect:***

***"They are cheaper than all other EC2 options" is incorrect.*** Spot, Savings Plans, and Reserved instances are all cheaper than On-Demand instances.

***"They only require 1-2 days for setup and configuration" is incorrect.*** You can configure and launch your EC2 instances in minutes.

***"They provide free capacity when testing your new applications" is incorrect.*** There is no free capacity for application testing. You can only have specific types of instances for free during the free tier period (12 months).

**References**:

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

Bottom of Form

Top of Form

Question 36:

**Skipped**

Which of the following services is used when encrypting EBS volumes?

* 

Amazon Macie

* 

AWS KMS

**(Correct)**

* 

AWS WAF

* 

Amazon GuardDuty

**Explanation**

             Amazon EBS encryption offers a straight-forward encryption solution for your EBS volumes that does not require you to build, maintain, and secure your own key management infrastructure. You can configure Amazon EBS to use the AWS Key Management Service (AWS KMS) to create and control the encryption keys used to encrypt your data. AWS Key Management Service is also integrated with other AWS services including Amazon S3, and Amazon Redshift, to make it simple to encrypt and decrypt your data.

***The other options are incorrect:***

***"Amazon GuardDuty" is incorrect.***Amazon GuardDuty offers **threat detection** that enables you to continuously monitor and protect your AWS accounts and workloads. GuardDuty analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.

***"AWS WAF" is incorrect.*** AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

***"Amazon Macie" is incorrect.*** Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data stored in Amazon S3. Macie automatically detects a large and growing list of sensitive data types, including personally identifiable information (PII) such as names, addresses, and credit card numbers. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with other AWS accounts. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data. Amazon Macie can also be used in combination with other AWS services, such as AWS Step Functions to take automated remediation actions. This can help you meet regulations, such as the General Data Privacy Regulation (GDPR).

**References:**

<https://aws.amazon.com/kms/>

<https://aws.amazon.com/ebs/faqs/>

Bottom of Form

Top of Form

Question 37:

**Skipped**

Amazon EC2 instances are conceptually very similar to traditional servers. However, using Amazon EC2 server instances in the same manner as traditional hardware server instances is only a starting point. What are the main benefits of using the AWS EC2 instances instead of traditional servers? (Choose TWO)

* 

Improves Fault-Tolerance

**(Correct)**

* 

Can be scaled manually in a shorter period of time

**(Correct)**

* 

Prevents unauthorized users from getting into your network

* 

Provides automatic data backups

* 

Provides your business with a seamless remote accessibility

**Explanation**

**"Improves Fault-Tolerance" is a correct answer.** AWS has unique set of services that you can use to build fault-tolerant applications in the cloud. For example you can get improved fault tolerance by placing your compute instances behind an Elastic Load Balancer, as it can automatically balance traffic across multiple instances and multiple Availability Zones and ensure that only healthy Amazon EC2 instances receive traffic.

         You can setup an Elastic Load Balancer to balance incoming application traffic across Amazon EC2 instances in a single Availability Zone or multiple Availability Zones. Elastic Load Balancing can detect the health of Amazon EC2 instances. When it detects unhealthy Amazon EC2 instances, it no longer routes traffic to those unhealthy instances. Instead, it spreads the load across the remaining healthy instances. If all of your Amazon EC2 instances in a particular Availability Zone are unhealthy, but you have set up instances in multiple Availability Zones, Elastic Load Balancing will route traffic to your healthy Amazon EC2 instances in those other zones. It will resume load balancing to the original Amazon EC2 instances when they have been restored to a healthy state.

        Also, using Auto Scaling enables you to reduce the amount of time and resources you need to monitor your servers – if a failure occurs, a replacement will be automatically launched for you. Diagnosing an unhealthy server can be as simple as terminating it and letting Auto Scaling launch a new one for you.

**"Can be scaled manually in a shorter period of time" is a correct answer.** Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity (manually or automatically), both up and down, as your computing requirements change.

***The other options are incorrect:***

***"Provides your business with a seamless remote accessibility" is incorrect.*** Both Amazon EC2 instances and traditional servers can provide access from any geographic area.

***"Prevents unauthorized users from getting into your network" is incorrect.*** Both AWS and on-premises include built-in firewall protection to help prevent unauthorized users from getting into your network.

***"Provides automatic data backups" is incorrect.*** Both AWS and on-premises provide automatic data backups to prevent data losses.

**References:**

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

<https://aws.amazon.com/ec2/>

Bottom of Form

Top of Form

Question 38:

**Skipped**

AWS provides disaster recovery capability by allowing customers to deploy infrastructure into multiple \_\_\_\_\_\_\_\_\_\_\_ .

* 

Support plans

* 

Edge locations

* 

Regions

**(Correct)**

* 

Transportation devices

**Explanation**

        Businesses are using the AWS cloud to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery architectures from “pilot light” environments that may be suitable for small customer workload data center failures to “hot standby” environments that enable rapid failover at scale. With data centers in Regions all around the world, AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of your IT infrastructure and data.

***The other options are incorrect:***

***"Transportation devices" is incorrect.***AWS uses storage transportation devices, like AWS Snowball and Snowmobile to allow companies transfer data to the cloud.

***"Support plans" is incorrect.***AWS provides multiple support plans to meet the different support requirements of its customers.

***"Edge locations" is incorrect.*** AWS edge locations are used by the CloudFront service to cache and serve content to end-users from a nearby geographical location to reduce latency.

**References:**

<https://aws.amazon.com/disaster-recovery/>

Bottom of Form

Top of Form

Question 39:

**Skipped**

A company is running a large web application that needs to alwaysbe available. The application tends to slow down when CPU usage is greater than 60%. How can they track when CPU usage goes above 60% for any of the EC2 Instances in their account?

* 

Use CloudWatch Alarms to monitor the CPU and alert when the CPU usage is >= 60%

**(Correct)**

* 

Set the AWS Config CPU threshold to 60% to receive a notification when EC2 usage exceeds that value

* 

Use SNS to monitor the utilization of the server

* 

Use CloudFront to monitor the CPU usage

**Explanation**

           Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring based on rules that you define. For example, you can monitor the CPU usage and disk reads and writes of your Amazon EC2 instances and then use this data to determine whether you should launch additional instances to handle increased load. You can also use this data to stop under-used instances to save money. In addition to monitoring the built-in metrics that come with AWS, you can monitor your own custom metrics. With CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health.

***The other options are incorrect:***

***"Use SNS to monitor the utilization of the server" is incorrect.***SNS is not used for monitoring. The service can be used in conjunction with CloudWatch to monitor and send notifications to your Email address. Using Amazon CloudWatch alarms, you can set up metric thresholds and send alerts to Amazon Simple Notification Service (SNS). SNS can send notifications using e-mail, HTTP(S) endpoints, and Short Message Service (SMS) messages to mobile phones.

***"Use CloudFront to monitor the CPU usage" is incorrect.***CloudFront is a Caching service that is used to deliver content to end users with low latency.

***"Set the AWS Config CPU threshold to 60% to receive a notification when EC2 usage exceeds that value" is incorrect.*** AWS Config cannot be used to monitor or set thresholds for your CPU usage. AWS Config enables you to review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

**References:**

<https://aws.amazon.com/cloudwatch/>

Bottom of Form

Top of Form

Question 40:

**Skipped**

What should you consider when storing data in Amazon Glacier?

* 

Attach Glacier to an EC2 Instance to be able to store data

* 

Amazon Glacier only accepts data in a compressed format

* 

Glacier can only be used to store frequently accessed data and data archives

* 

Amazon Glacier does not provide immediate retrieval of data

**(Correct)**

**Explanation**

          Objects stored in Glacier take time to retrieve. You can pay for expedited retrieval, which will take several minutes or wait several hours for normal retrieval.

***The other options are incorrect:***

***"Amazon Glacier only accepts data in a compressed format" is incorrect.*** You can store virtually any kind of data in any format. But your costs will be lower if you aggregate and compress your data.

***"Attach Glacier to an EC2 Instance to be able to store data" is incorrect.*** Glacier cannot be attached to EC2 instances. Glacier is a storage class of S3.

***"Glacier can only be used to store frequently accessed data and data archives" is incorrect.*** Glacier is not for frequently accessed data.

**References:**

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/how-aws-pricing-works.pdf>

Bottom of Form

Top of Form

Question 41:

**Skipped**

A company wants to use Amazon Elastic Container Service (Amazon ECS) to run its containerized applications. For compliance reasons, the company wants to retain complete visibility and control over the underlying server cluster. Which Amazon ECS launch type will satisfy these requirements?

* 

EC2 launch type

**(Correct)**

* 

Fargate launch type

* 

Lambda launch type

* 

Lightsail launch type

**Explanation**

      Amazon Elastic Container Service (Amazon ECS) has two modes: Fargate launch type (serverless) and EC2 launch type (server-based). The Fargate launch type allows you to run containers without having to manage servers or clusters. The EC2 launch type allows you to have server-level, more granular control over the infrastructure that runs your container applications.

***The other options are incorrect:***

***"Fargate launch type" is incorrect.***AWS customers who use AWS Fargate to run their containers do not have control over the underlying infrastructure. AWS Fargate is a **serverless** compute engine for Amazon ECS that allows customers to run containers without having to manage servers or clusters. AWS Fargate launch type is more suitable for customers who want to run containers without managing the underlying infrastructure.

***"Lambda launch type" and "Lightsail launch type" are incorrect.***Amazon ECS has only two modes: Fargate launch type (serverless) and EC2 launch type (server-based).

**References:**

<https://aws.amazon.com/ecs/>

Bottom of Form

Top of Form

Question 42:

**Skipped**

Which AWS service can be used to route end users to the nearest AWS Region to reduce latency?

* 

Amazon Cognito

* 

AWS Systems Manager Session Manager

* 

AWS Cloud9

* 

Amazon Route 53

**(Correct)**

**Explanation**

            Amazon Route 53 helps AWS Customers improve their application’s performance for a global audience. Amazon Route 53 latency-based policy routes user requests to the closest AWS Region, which reduces latency and improves application performance.

***The other options are incorrect:***

***"Amazon Cognito" is incorrect.***Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, Google or Apple.

***"AWS Systems Manager Session Manager" is incorrect.***AWS Systems Manager Session Manager does not route traffic. AWS Systems Manager Session Manager is an AWS Systems Manager capability that allows users to **connect** to an EC2 instance with just one click from the browser (or AWS CLI) **without having to provide SSH Key Pairs.** Session Manager helps you improve your security posture by letting you close SSH inbound ports, freeing you from managing SSH keys, and bastion hosts.

***"AWS Cloud9" is incorrect.*** AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser. It includes a code editor, debugger, and terminal. Cloud9 comes prepackaged with essential tools for popular programming languages, including JavaScript, Python, PHP, and more, so you don’t need to install files or configure your development machine to start new projects.

**References:**

<https://aws.amazon.com/route53/>

Bottom of Form

Top of Form

Question 43:

**Skipped**

Which AWS services allow users to run SQL queries against data stored in Amazon S3? (Choose TWO)

* 

Amazon RDS

* 

Amazon Redshift Spectrum

**(Correct)**

* 

AWS Shield

* 

Amazon Comprehend

* 

Amazon Athena

**(Correct)**

**Explanation**

      Amazon Athena is an analytics service that makes it easy to query data in Amazon S3 using standard SQL commands. With Athena, there’s no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets. Athena is serverless, so there is no infrastructure to setup or manage, and you can start analyzing your data immediately.

      Amazon Redshift Spectrum is a feature of Amazon Redshift that enables you to run SQL queries against exabytes of data in Amazon S3, with no loading or ETL required. This enables you to use your data to acquire new insights for your business and customers.

***The other options are incorrect:***

***"Amazon RDS" is incorrect.*** Amazon Relational Database Service (Amazon RDS) is used to set up and operate a relational database in the cloud.

***“Amazon Comprehend” is incorrect.*** Amazon Comprehend is a **Natural Language Processing (NLP) service** that uses machine learning to find meaning and insights in text. Customers can use Amazon Comprehend to identify the language of the text, extract key phrases, places, people, brands, or events, understand sentiment about products or services, and identify the main topics from a library of documents. The source of this text could be web pages, social media feeds, emails, or articles. Amazon Comprehend is fully managed, so there are no servers to provision, and no machine learning models to build, train, or deploy.

**Note: Natural language processing (NLP) is an artificial intelligence technology that helps computers identify, understand, and manipulate human language.**

***"AWS Shield" is incorrect.***AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers and provides always-on detection and automatic inline mitigations that minimize application downtime and latency.

**References:**

<https://aws.amazon.com/athena/>

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

Bottom of Form

Top of Form

Question 44:

**Skipped**

A financial services company decides to migrate one of its applications to AWS. The application deals with sensitive data, such as credit card information, and must run on a PCI-compliant environment. Which of the following is the company’s responsibility when building a PCI-compliant environment in AWS? (Choose TWO)

* 

Restrict any access to cardholder data and create a policy that addresses information security for all personnel

**(Correct)**

* 

Ensure that all PCI DSS physical security requirements are met

* 

Configure the underlying infrastructure of AWS services to meet all PCI DSS requirements

* 

Start the migration process immediately as all AWS services are PCI compliant

* 

Ensure that AWS services are configured properly to meet all PCI DSS standards

**(Correct)**

**Explanation**

     The Payment Card Industry Data Security Standard (PCI DSS) helps ensure that companies maintain a secure environment for storing, processing, and transmitting credit card information or sensitive authentication data (SAD). AWS customers who use AWS services to store, process, or transmit cardholder data can rely on AWS infrastructure as they manage their own PCI DSS compliance certification.

     Security and compliance are important shared responsibilities between AWS and the customer. It is the customer’s responsibility to maintain their PCI DSS cardholder data environment (CDE) and scope, and be able to demonstrate compliance of all PCI controls, but customers are not alone in this journey. The use of PCI DSS compliant AWS services can facilitate customer compliance, and the AWS Security Assurance Services team can assist customers with additional information specific to demonstrating the PCI DSS compliance of their AWS workloads.

     AWS Services listed as PCI DSS compliant means that they can be configured by customers to meet their PCI DSS requirements. It does not mean that any use of that service is automatically compliant. A good rule-of-thumb is that if a customer can set a particular configuration, they are responsible for setting it appropriately to meet PCI DSS requirements. AWS customers are also responsible for creating a policy that addresses information security for all personnel, and implementing strong access controls to restrict any access to cardholder data.

***The other options are incorrect:***

***“Ensure that all PCI DSS physical security requirements are met” is incorrect.***AWS is responsible for the security and compliance of its physical infrastructure, including the PCI DSS requirements.

***“Start the migration process immediately as all AWS services are PCI compliant” is incorrect.***Only certain AWS services are in-scope for PCI compliance. You can find a full list of in-scope services here. https://aws.amazon.com/compliance/services-in-scope/

***“Configure the underlying infrastructure of AWS services to meet all applicable requirements of PCI DSS” is incorrect.***Configuring the underlying infrastructure of AWS services is the responsibility of AWS, not the customer. If a customer is using one of the services that are in-scope for PCI DSS, the entire infrastructure that supports these services is compliant.

**References:**

<https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf>

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

Bottom of Form

Top of Form

Question 45:

**Skipped**

How does AWS help customers achieve compliance in the cloud?

* 

AWS has many common assurance certifications such as ISO 9001 and HIPAA

**(Correct)**

* 

AWS applies the most common Cloud security standards, and is responsible for complying with customers’ applicable laws and regulations

* 

Many AWS services are assessed regularly to comply with local laws and regulations

* 

It’s not possible to meet regulatory compliance requirements in the Cloud

**Explanation**

       AWS environments are continuously audited, and its infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries, including PCI DSS, ISO 2700, ISO 9001, and HIPAA. You can use these certifications to validate the implementation and effectiveness of AWS security controls. For example, AWS companies that use AWS products and services to handle credit card information can rely on AWS technology infrastructure as they manage their PCI DSS compliance certification.

***The other options are incorrect:***

***"AWS applies the most common Cloud security standards, and is responsible for complying with customers’ applicable laws and regulations" is incorrect.***In all cases, customers operating in the cloud remain responsible for complying with applicable laws and regulations.

***"Many AWS services are assessed regularly to comply with local laws and regulations" is incorrect.*** AWS services are assessed regularly to comply with common compliance standards NOT with local laws and regulations.

***"It’s not possible to meet regulatory compliance requirements in the Cloud" is incorrect.***AWS environments are continuously audited, and its infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. For example, AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) to use the secure AWS environment to process, maintain, and store protected health information.

**References:**

<https://d0.awsstatic.com/whitepapers/compliance/AWS_Compliance_Quick_Reference.pdf>

Bottom of Form

Top of Form

Question 46:

**Skipped**

How can you protect data stored on Amazon S3 from accidental deletion?

* 

By configuring S3 Lifecycle Policies

* 

By disabling S3 Cross-Region Replication (CRR)

* 

By configuring S3 Bucket Policies

* 

By enabling S3 Versioning

**(Correct)**

**Explanation**

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

     Versioning-enabled buckets can help you recover objects from accidental deletion or overwrite. For example, if you delete an object, instead of removing it permanently, Amazon S3 inserts a delete marker, which becomes the current object version. Also, If you overwrite an object, it results in a new object version in the bucket. You can always restore the previous version.

***The other options are incorrect:***

***“By disabling S3 Cross-Region Replication (CRR)” is incorrect***. S3 Cross-Region Replication (CRR) is an Amazon S3 feature that enables customers to replicate data across different AWS Regions; to minimize latency for global users and\or meet compliance requirements. Disabling S3 Cross-Region Replication (CRR) does not help protect data from accidental deletion.

***“By configuring S3 lifecycle policies” is incorrect.***With S3 Lifecycle configuration rules, you can tell Amazon S3 to transition objects to less expensive storage classes, or archive or delete them. In order to reduce your Amazon S3 costs, you should create a lifecycle policy to automatically move old (or infrequently accessed) files to less expensive storage tiers, or to automatically delete them after a specified duration. The S3 Lifecycle feature is not meant to protect from accidental deletion of data.

***“By configuring S3 Bucket Policies” is incorrect.***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. A Bucket Policy defines who can access a bucket, but does not help if an authorized user accidentally deleted objects in that bucket.

**References:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>

Bottom of Form

Top of Form

Question 47:

**Skipped**

For some services, AWS automatically replicates data across multiple Availability Zones to provide fault tolerance in the event of a server failure or Availability Zone outage. Select TWO services that automatically replicate data across Availability Zones.

* 

Amazon Aurora

**(Correct)**

* 

Amazon Route 53

* 

Amazon RDS for Oracle

* 

Instance Store

* 

S3

**(Correct)**

**Explanation**

      For S3 Standard, S3 Standard-IA, and S3 Glacier storage classes, your objects are automatically stored across multiple devices spanning a minimum of three Availability Zones, each on different power grids within an AWS Region. This means your data is available when needed and protected against AZ failures.

      Amazon Aurora is an Amazon RDS database engine. All of your data in Amazon Aurora is automatically replicated across three Availability Zones within an AWS region, providing built-in high availability and data durability.

      Other Amazon RDS database engines (PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server) do not replicate data automatically. To protect from data loss when using any of these engines, you need to manually enable the Multi-AZ feature. In a Multi-AZ Deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. If you encounter problems with the primary copy, Amazon RDS automatically switches to the standby copy to provide continued availability to the data.

***The other options are incorrect:***

***"Instance Store" is incorrect.***An instance store provides temporary block-level storage for EC2 instances. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content.

***"Amazon Route 53" is incorrect.***Amazon Route 53 is not used for storing data. It is a globally available, cloud-based Domain Name System (DNS) web service not tied to Availability Zones.

***"Amazon RDS for Oracle" is incorrect.***Amazon RDS for Oracle does not automatically replicate data. Amazon RDS supports six database engines (Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server). Amazon Aurora is the only database engine that replicates data automatically across three Availability Zones. For other database engines, you must enable the "Multi-AZ" feature manually. In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a standby copy of your data in a different Availability Zone. If a storage volume on your primary instance fails, Amazon RDS automatically initiates a failover to the up-to-date standby.

**References:**

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

<https://aws.amazon.com/s3/faqs/>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

Bottom of Form

Top of Form

Question 48:

**Skipped**

A company needs to host a big data application on AWS using EC2 instances. Which of the following AWS Storage services would they choose to automatically get high throughput to multiple compute nodes?

* 

Amazon Elastic Block Store

* 

S3

* 

AWS Storage Gateway

* 

Amazon Elastic File System

**(Correct)**

**Explanation**

       Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It offers a simple interface that allows you to create and configure file systems quickly and easily. Amazon EFS is built to elastically scale on demand without disrupting applications, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it.

      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 that scale as a file system grows, with consistent low latencies. As a regional service, Amazon EFS is designed for high availability and durability storing data redundantly across multiple Availability Zones. With these capabilities, Amazon EFS is well suited to support a broad spectrum of use cases, including web serving and content management, enterprise applications, media and entertainment processing workflows, home directories, database backups, developer tools, container storage, and big data analytics workloads.

***The other options are incorrect:***

***Amazon Elastic Block Store is incorrect.*** An Amazon Elastic Block Store volume cannot be attached to multiple compute resources at a time.

***S3 is incorrect.*** S3 is an object level storage. S3 cannot be attached to compute resources.

***AWS Storage Gateway is incorrect.***AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. You can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration.

**References:**

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

Bottom of Form

Top of Form

Question 49:

**Skipped**

According to the AWS shared responsibility model, what are the controls that customers fully inherit from AWS? (Choose TWO)

* 

Resource Configuration Management

* 

Awareness and Training

* 

Data center security controls

**(Correct)**

* 

Communications controls

* 

Environmental controls

**(Correct)**

**Explanation**

**AWS is responsible** for physical controls and environmental controls. Customers inherit these controls from AWS.

        As mentioned in the [AWS Shared Responsibility Model page](https://aws.amazon.com/compliance/shared-responsibility-model/), Inherited Controls are controls which a customer fully inherits from AWS such as physical controls and environmental controls.

        As a customer deploying an application on AWS infrastructure, you inherit security controls pertaining to the AWS physical, environmental and media protection, and no longer need to provide a detailed description of how you comply with these control families.

        For example: You have built an application in AWS for customers to securely store their data, but your customers are concerned about the security of the data and ensuring compliance requirements are met. To address this, you assure your customer that “our company does not host customer data in its corporate or remote offices, but rather in AWS data centers that have been certified to meet industry security standards.” That includes physical and environmental controls to secure the data, which is the responsibility of Amazon. Customers of AWS do not have physical access to the AWS data centers, and as such, they fully inherit the physical and environmental security controls from AWS.

You can read more about AWS’ data center controls here:

<https://aws.amazon.com/compliance/data-center/controls/>

***The other options are incorrect:***

***"Communications controls" is incorrect.*** Communications controls are the responsibility of the customer.

***"Awareness and Training" is incorrect.***Awareness and Training belongs to the **AWS** **Shared Controls**. AWS trains AWS employees, but a customer must train their own employees.

***"Resource Configuration Management" is incorrect.***Configuration management belongs to the **AWS Shared Controls**. AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

**References:**

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

Bottom of Form

Top of Form

Question 50:

**Skipped**

Which of the following makes it easier for you to categorize**,**manage and filter your resources?

* 

AWS Tagging

**(Correct)**

* 

AWS Service Catalog

* 

AWS Directory Service

* 

Amazon CloudWatch

**Explanation**

              Amazon Web Services (AWS) allows customers to assign metadata to their AWS resources in the form of tags. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. Although there are no inherent types of tags, they enable customers to categorize resources by purpose, owner, environment, or other criteria.

***The other options are incorrect:***

***AWS Directory Service is incorrect.*** AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

***Amazon CloudWatch is incorrect.*** Amazon CloudWatch is a monitoring service for resource utilization.

***AWS Service Catalog is incorrect.*** AWS Service Catalog is not used to filter your resources. It is used to create and manage catalogs of IT services that are approved for use on AWS. This helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

**References:**

<https://aws.amazon.com/answers/account-management/aws-tagging-strategies/>

Bottom of Form

Top of Form

Question 51:

**Skipped**

Which of the following services enables you to easily generate and use your own encryption keys in the AWS Cloud?

* 

AWS WAF

* 

AWS CloudHSM

**(Correct)**

* 

AWS Shield

* 

AWS Certificate Manager

**Explanation**

              AWS CloudHSM is a cloud-based Hardware Security Module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

***The other options are incorrect:***

***"AWS Certificate Manager" is incorrect.*** AWS Certificate Manager is a service that lets you provision, manage, and deploy (SSL/TLS) certificates for use with AWS services and your internal connected resources.

***"AWS Shield" is incorrect.***AWS Shield is a managed Distributed Denial of Service (DDoS) protection service.

***"AWS WAF" is incorrect.***AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

**References:**

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>    page 58

Bottom of Form

Top of Form

Question 52:

**Skipped**

Which of the following security resources are available to any user for free? (Choose TWO)

* 

AWS TAM

* 

AWS Classroom Training

* 

AWS Security Blog

**(Correct)**

* 

AWS Bulletins

**(Correct)**

* 

AWS Support API

**Explanation**

         The AWS free security resources include the AWS Security Blog, Whitepapers, AWS Developer Forums, Articles and Tutorials, Training, Security Bulletins, Compliance Resources and Testimonials.

**The other options are incorrect.**

***"AWS Classroom Training" is incorrect***. AWS provides live classes (Classroom Training) with accredited AWS instructors who teach you in-demand cloud skills and best practices using a mix of presentations, discussion, and hands-on labs. AWS Classroom Training is not free.

***"AWS Support API" is incorrect.***AWS Support API is available only for AWS  customers who have a **Business** or **Enterprise** support plan. The AWS Support API provides **programmatic access** to AWS Support Center features to create, manage, and close support cases.

***"AWS TAM" is incorrect.*** A Technical Account Manager (TAM) is your designated technical point of contact who provides advocacy and guidance to help plan and build solutions using best practices and proactively keep your AWS environment operationally healthy and secure. TAM is available only for the **Enterprise** support plan.

**References:**

<https://aws.amazon.com/security/security-bulletins/>

<https://aws.amazon.com/blogs/security/>

Bottom of Form

Top of Form

Question 53:

**Skipped**

Each AWS Region is composed of multiple Availability Zones. Which of the following best describes what an Availability Zone is?

* 

It is a distinct location within a region that is insulated from failures in other Availability Zones

**(Correct)**

* 

It is a collection of data centers distributed in multiple countries

* 

It is a collection of Local Zones designed to be completely isolated from each other

* 

It is a logically isolated network of the AWS Cloud

**Explanation**

               Availability Zones are distinct locations within a region that are insulated from failures in other Availability Zones.

Note:

Although Availability Zones are insulated from failures in other Availability Zones,  they are connected through private, low-latency links to other Availability Zones in the same region.

***The other options are incorrect:***

***"It is a collection of data centers distributed in multiple countries" is incorrect.*** An Availability Zone is a collection of data centers located in one AWS Region.

***"It is a logically isolated network of the AWS Cloud" is incorrect.*** This statement describes Amazon VPC.

***"It is a collection of Local Zones designed to be completely isolated from each other" is incorrect.*** An Availability Zone consists of one or more discrete **data centers** located in one AWS Region.

[**A Local Zone**](https://aws.amazon.com/about-aws/global-infrastructure/localzones/)**is an extension of an AWS Region in geographic proximity to your users.** With AWS Local Zones, you can easily run highly-demanding applications that require single-digit millisecond latencies to your end-users, such as real-time gaming, hybrid migrations, AR/VR, and machine learning. AWS Local Zones enable you to comply with state and local data residency requirements in sectors such as healthcare, financial services, iGaming, and government.

AWS Local Zones are connected to the parent region via Amazon’s redundant and very high bandwidth private network, giving applications running in AWS Local Zones fast, secure, and seamless access to the full range of in-region services through the same APIs and tool sets.

**References:**

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

Bottom of Form

Top of Form

Question 54:

**Skipped**

What is the main benefit of attaching security groups to an Amazon RDS instance?

* 

Manages user access and encryption keys

* 

Distributes incoming traffic across multiple targets

* 

Controls what IP address ranges can connect to your database instance

**(Correct)**

* 

Deploys SSL/TLS certificates for use with your database instance

**Explanation**

              In Amazon RDS, security groups are used to control which IP address ranges can connect to your databases on a DB instance. When you initially create a DB instance, its firewall prevents any database access except through rules specified by an associated security group.

**References:**

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.html>

Bottom of Form

Top of Form

Question 55:

**Skipped**

What can you access by visiting the URL: http://status.aws.amazon.com?

* 

AWS Security Dashboard

* 

AWS Billing Dashboard

* 

AWS Cost Dashboard

* 

AWS Service Health Dashboard

**(Correct)**

**Explanation**

        The AWS Service Health Dashboard publishes AWS’ most up-to-the-minute information on service availability. The dashboard provides access to current status and historical data about every AWS Service.

**References:**

<http://status.aws.amazon.com/>

Bottom of Form

Top of Form

Question 56:

**Skipped**

You are working as a site reliability engineer (SRE) in an AWS environment, which of the following services helps monitor your applications?

* 

Amazon CloudWatch

**(Correct)**

* 

Amazon Elastic MapReduce

* 

Amazon CloudSearch

* 

Amazon CloudHSM

**Explanation**

             Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications  running on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.

**The other options are incorrect:**

***Amazon Elastic MapReduce is incorrect.*** Amazon Elastic MapReduce (Amazon EMR) provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances.

***Amazon CloudSearch is incorrect.***Amazon CloudSearch is used to set up, manage, and scale a search solution for your website or application.

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

**References:**

<https://aws.amazon.com/cloudwatch/>

Bottom of Form

Top of Form

Question 57:

**Skipped**

What AWS service allows you to buy third-party software solutions and services that run on AWS resources?

* 

Resource Groups

* 

AWS Application Discovery service

* 

AWS Marketplace

**(Correct)**

* 

Amazon DevPay

**Explanation**

           The AWS Marketplace is a curated digital catalog that makes it easy for customers to find, buy, deploy, and manage third-party software and services that customers need to build solutions and run their businesses. The AWS Marketplace includes thousands of software listings from popular categories such as security, networking, storage, machine learning, business intelligence, database, and DevOps. The AWS Marketplace also simplifies software licensing and procurement with flexible pricing options and multiple deployment methods. Customers can quickly launch pre-configured software with just a few clicks, and choose software solutions in AMI and SaaS formats, as well as other formats. Flexible pricing options include free trial, hourly, monthly, annual, multi-year, and BYOL.

***The other options are incorrect:***

***"AWS Application Discovery Service" is incorrect.***AWS Application Discovery Service helps AWS customers quickly and reliably plan application migration projects by automatically identifying applications running in on-premises data centers, their associated dependencies, and their performance profiles.

      Planning data center migrations can involve thousands of workloads that are often deeply interdependent. Application discovery and dependency mapping are important early first steps in the migration process, but these tasks are difficult to perform at scale due to the lack of automated tools. AWS Application Discovery Service automatically collects configuration and usage data from servers, storage, and networking equipment to develop a list of applications, how they perform, and how they are interdependent. This information helps reduce the complexity and time in planning your cloud migration.

***"Resource Groups" is incorrect.***Resource Groups help you organize multiple AWS resources in groups. By default, the AWS Management Console is organized by AWS service. But with the Resource Groups tool, you can create a custom console that organizes and consolidates information based on your project and the resources that you use.

***"Amazon DevPay" is incorrect.***Amazon DevPay is a cloud-based billing and account management service that enables developers to collect payment for their AWS applications. Note: AWS may stop this service soon. The service is not accepting new seller accounts.

**References:**

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

Bottom of Form

Top of Form

Question 58:

**Skipped**

Which of the following is the responsibility of AWS according to the AWS Shared Responsibility Model?

* 

Performing auditing tasks

* 

Securing regions and edge locations

**(Correct)**

* 

Monitoring AWS resources usage

* 

Securing access to AWS resources

**Explanation**

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

***All other options represent responsibilities of the customer.***

**References:**

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

Bottom of Form

Top of Form

Question 59:

**Skipped**

Engineers are wasting a lot of time and effort managing batch computing software in traditional data centers. Which of the following AWS services allows them to easily run thousands of batch computing jobs?

* 

AWS Fargate

* 

Amazon EC2

* 

AWS Batch

**(Correct)**

* 

Lambda@Edge

**Explanation**

          AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory-optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. With AWS Batch, there is no need to install and manage batch computing software or server clusters that you use to run your jobs, allowing you to focus on analyzing results and solving problems. AWS Batch plans, schedules, and executes your batch computing workloads across the full range of AWS compute services and features, such as Amazon EC2 and Spot Instances.

***The other options are incorrect:***

***Amazon EC2 is incorrect.***Amazon EC2 can be used to run any number of batch processing jobs but you are responsible for installing and managing a batch computing software and creating the server clusters.

***AWS Fargate is incorrect.***AWS Fargate is a compute engine for Amazon ECS that allows you to run containers without having to manage servers or clusters.

***Lambda@Edge is incorrect.*** Lambda@Edge is a feature of Amazon CloudFront that lets you run code closer to your global end-users, which improves performance and reduces latency.

**References:**

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>         page 20

Bottom of Form

Top of Form

Question 60:

**Skipped**

Which pillar of the AWS Well-Architected Framework provides recommendations to help customers select the right compute resources based on workload requirements?

* 

Reliability

* 

Operational Excellence

* 

Security

* 

Performance Efficiency

**(Correct)**

**Explanation**

        The AWS Well-Architected Framework describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud.

The five Pillars of the AWS Well-Architected Framework: (IMPORTANT)

1- Operational Excellence

2- Security

3- Reliability

4- Performance Efficiency

5- Cost Optimization

The correct answer is: Performance Efficiency

       The performance efficiency pillar includes the ability to use computing resources efficiently to meet system requirements. 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.

***The other options are incorrect:***

***"Reliability" is incorrect.***The reliability pillar includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. A resilient workload quickly recovers from failures to meet business and customer demand. Key topics include distributed system design, recovery planning, and how to handle change.

***"Operational Excellence" is incorrect.***The operational excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

***"Security" is incorrect.***The security pillar includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies. 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.

**References:**

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

Bottom of Form

Top of Form

Question 61:

**Skipped**

You have developed a web application targeting a global audience. Which of the following will help you achieve the highest redundancy and fault tolerance from an infrastructure perspective?

* 

Deploy the application in multiple Availability Zones in a single AWS region

* 

There is no need to architect for these capabilities in AWS, as AWS is redundant by default

* 

Deploy the application in a single Availability Zone

* 

Deploy the application in multiple Availability Zones in multiple AWS regions

**(Correct)**

**Explanation**

       Since you are targeting a global audience, you should leverage AWS global regions to serve content to your users. The deployment option that gives you the highest redundancy is to deploy the application in multiple Availability Zones within multiple AWS regions. This redundancy will also increase the fault tolerance of the application because if there is an outage in a single Availability Zone, the other Availability Zones can handle requests.

**Additional information:**

       It is important to understand that the AWS Cloud infrastructure is built around Regions and Availability Zones (AZs). A Region is a geographical location that contains multiple Availability Zones. Each AWS Region is designed to be completely isolated from the other AWS Regions. This achieves the greatest possible fault tolerance and stability.

       An Availability Zone is a data center, or data centers, that are completely isolated from the other Availability Zones. Each AWS Region has at least two Availability Zones; most have three. Each Availability Zone is engineered to be independent from failures in other Availability Zones. Deploying your resources across multiple Availability Zones offer you the ability to operate production applications and databases that are more resilient, highly available, and scalable than would be possible from a single data center.

**References:**

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

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

Bottom of Form

Top of Form

Question 62:

**Skipped**

Which of the following is NOT a benefit of using AWS Lambda?

* 

There is no charge when your AWS Lambda code is not running

* 

AWS Lambda runs code without provisioning or managing servers

* 

AWS Lambda provides resizable compute capacity in the cloud

**(Correct)**

* 

AWS Lambda can be called directly from any mobile app

**Explanation**

***"AWS Lambda provides resizable compute capacity in the cloud"****is not a benefit of AWS Lambda, so is the correct choice.* AWS Lambda automatically runs your code without requiring you to adjust capacity or manage servers. AWS Lambda automatically scales your application by running code in response to each trigger. Your code runs in parallel and processes each trigger individually, scaling precisely with the size of the workload.

***Other options represent benefits of AWS Lambda, so are not correct.*** AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume—there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service—all with zero administration. Just upload your code, and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services, or you can call it directly from any web or mobile app.

**References:**

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

Bottom of Form

Top of Form

Question 63:

**Skipped**

Which of the following is a benefit of the "Loose Coupling" architecture principle?

* 

It allows for Cross-Region Replication

* 

It helps AWS customers reduce Privileged Access to AWS resources

* 

It allows individual application components or services to be modified without affecting other components

**(Correct)**

* 

It eliminates the need for change management

**Explanation**

             As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components. This means that IT systems should be designed in a way that reduces interdependencies - a change or a failure in one component should not cascade to other components.

**The AWS services that can help you build loosely-coupled applications include:**

**1- Amazon Simple Queue Service (Amazon SQS):**Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS offers a reliable, highly-scalable hosted queue for storing messages as they travel between applications or microservices. It moves data between distributed application components and helps you decouple these components.

**2- Amazon EventBridge (also called Amazon CloudWatch Events):**Amazon EventBridge is a serverless event bus service that makes it easy for you to build event-driven application architectures. Amazon EventBridge helps you accelerate modernizing and re-orchestrating your architecture with decoupled services and applications. With EventBridge, you can speed up your organization’s development process by allowing teams to iterate on features without explicit dependencies between systems.

**3- Amazon SNS:** Amazon SNS is a publish/subscribe messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Both Amazon SNS and Amazon EventBridge can be used to implement the publish-subscribe pattern. Amazon EventBridge includes direct integrations with software as a service (SaaS) applications and other AWS services. It’s ideal for publish-subscribe use cases involving these types of integrations.

***The other options are incorrect:***

***"It helps AWS customers reduce Privileged Access to AWS resources" is incorrect.***This statement is related to the "Principle of Lease Privilege", not "Loose Coupling". Loose Coupling does not deal with access privileges.

***"It allows for Cross-Region Replication" is incorrect.***There is no relation between Cross-Region Replication and Loose Coupling. Cross-Region Replication (CRR) is an Amazon S3 feature that enables customers to replicate data across different AWS Regions; to minimize latency for global users and\or meet compliance requirements.

***"It eliminates the need for change management" is incorrect.***Loose Coupling does not eliminate the need for Change Management. Change Management is the process responsible for controlling the Lifecycle of all Changes made in an AWS account. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT Services. An erroneous configuration or misstep in a process can frequently lead to infrastructure or service disruptions. Creating and implementing a change management strategy will help reduce the risk of failure by monitoring all changes and rolling back failed changes.

Additional information:

AWS Config and AWS CloudTrail are change management tools that help AWS customers audit and monitor all resource and configuration changes in their AWS environment. AWS Config provides information about the changes made to a resource, and AWS CloudTrail provides information about who made those changes. These capabilities enable customers to discover any misconfigurations, fix them, and protect their workloads from failures.

**References:**

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

Bottom of Form

Top of Form

Question 64:

**Skipped**

What factors determine how you are charged when using AWS Lambda? (Choose TWO)

* 

Number of volumes

* 

Number of requests to your functions

**(Correct)**

* 

Storage consumed

* 

Placement groups

* 

Compute time consumed

**(Correct)**

**Explanation**

          With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the time it takes for your code to execute.

***The other options are incorrect:***

***"Placement groups"is incorrect.*** Placement Groups are logical groupings or clusters of EC2 instances within a single Availability Zone.

***"Storage consumed" and "Number of volumes" are incorrect.*** Lambda is not a storage service. It is a compute service to run your applications.

**References:**

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/how-aws-pricing-works.pdf>   page 11

Bottom of Form

Top of Form

Question 65:

**Skipped**

Which of the following AWS services integrates with AWS Shield and AWS Web Application Firewall (AWS WAF) to protect against network and application layer DDoS attacks?

* 

Amazon CloudFront

**(Correct)**

* 

AWS Secrets Manager

* 

Amazon EFS

* 

AWS Systems Manager

**Explanation**

      Amazon CloudFront, AWS Shield, and AWS Web Application Firewall (AWS WAF) work seamlessly together to create a flexible, layered security perimeter against multiple types of attacks including network and application layer DDoS attacks. These services are co-resident at the AWS edge location and provide a scalable, reliable, and high-performance security perimeter for your applications and content.

      All CloudFront distributions are defended by default against the most frequently occurring DDoS attacks that target your websites or applications with AWS Shield Standard. To defend against more complex attacks, you can add a flexible, layered security perimeter by integrating CloudFront with AWS Shield Advanced and AWS Web Application Firewall (AWS WAF).

Additional information:

      AWS Shield provides always-on DDoS detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications.

***The other options are incorrect:***

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

Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage your infrastructure at scale.

***"AWS Secrets Manager" is incorrect.***AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

***"Amazon EFS" is incorrect.***Amazon EFS is a storage service.

**References:**

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

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

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

Bottom of Form