AWS Practitioner

Question 1:

Skipped

A company is concerned that they are spending money on underutilized compute resources in AWS. Which AWS feature will help ensure that their applications are automatically adding/removing EC2 compute capacity to closely match the required demand?

- **AWS Cost Explorer**
- **AWS Elastic Load Balancer**
- **AWS Budgets**
- **AWS Auto Scaling**

  (Correct)

Explanation

AWS Auto Scaling is the feature that automates the process of adding/removing server capacity (based on demand). Autoscaling allows you to reduce your costs by automatically turning off resources that aren't in use. On the other hand, Autoscaling ensures that your application runs effectively by provisioning more server capacity if required.

The other options are incorrect:

"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.

"AWS Elastic Load Balancer" is incorrect. AWS Elastic Load Balancer (ELB) is a service that distributes the incoming application traffic to multiple targets that you define.

"AWS Cost Explorer" is incorrect. AWS Cost Explorer provides an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time.

References:

https://aws.amazon.com/autoscaling/

Question 2:

Skipped

What are the benefits of having infrastructure hosted in AWS? (Choose TWO)

- **Gaining complete control over the physical infrastructure**
- **Operating applications on behalf of customers**
- **All of the physical security and most of the data/network security are taken care of for you**

  (Correct)

- **Increasing speed and agility**

  (Correct)

- **There is no need to worry about security**

Explanation

All of the physical security are taken care of for you. Amazon data centers are surrounded by three physical layers of security. “Nothing can go in or out without setting off an alarm”. It’s important to keep bad guys out, but equally important to keep the data in which is why Amazon monitors incoming gear, tracking every disk that enters the facility. And “if it breaks we don’t return the disk for warranty. The only way a disk leaves our data center is when it’s confetti.”

Most (not all) data and network security are taken care of for you. When we talk about the data/network security, AWS has a “shared responsibility model” where AWS and the customer share the responsibility of securing them. For example, the customer is responsible for creating rules to secure their network traffic using the security groups and is also responsible for protecting data with encryption.

"Increasing speed and agility" is also a correct answer because in a cloud computing environment, new IT resources are only a click away, which means it requires less time to make those resources available to developers - from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

The other options are incorrect:

"Gaining complete control over the physical infrastructure" is incorrect. The Physical infrastructure is a responsibility of AWS, not the customer.

"Operating applications on behalf of customers" is incorrect. AWS customers are responsible for building and operating their applications.

"There is no need to worry about security" is incorrect. As mentioned above, security is a shared responsibility between AWS and the customer. For example, the customer has to manage who can access and use AWS resources using the IAM service.

References:

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

Question 3:

Skipped

Which of the following helps a customer view the Amazon EC2 billing activity for the past month?

- **AWS Systems Manager**
- **AWS Budgets**
- **AWS Cost & Usage Reports**

  (Correct)

- **AWS Pricing Calculator**

Explanation

The AWS Cost & Usage Report is your one-stop shop for accessing the most detailed information available about your AWS costs and usage.The AWS Cost & Usage Report lists AWS usage for each service category used by an account and its IAM users in hourly or daily line items, as well as any tags that you have activated for cost allocation purposes.

The other options are incorrect:

"AWS Pricing Calculator" is incorrect. AWS Pricing Calculator is a web service that you can use to estimate the cost for your AWS monthly bill based on your expected usage.

"AWS Systems Manager" is incorrect. 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.

"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/aws-cost-management/aws-cost-and-usage-reporting/

Question 4:

Skipped

What does AWS Snowball provide? (Choose TWO)

- **Secure transfer of large amounts of data into and out of the AWS Cloud**

  (Correct)

- **A hybrid cloud storage between on-premises environments and the AWS Cloud**
- **Built-in computing capabilities that allow customers to process data locally**

  (Correct)

- **A catalog of third-party software solutions that customers need to build solutions and run their businesses**
- **An Exabyte-scale data transfer service that allows you to move extremely large amounts of data to AWS**

Explanation

AWS Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers, including high network costs, long transfer times, and security concerns. AWS Customers use Snowball to migrate analytics data, genomics data, video libraries, image repositories, and backups. Transferring data with Snowball is simple, fast, secure, and can cost as little as one-fifth the cost of using high-speed internet.

Additionally, With AWS Snowball, you can access the compute power of the AWS Cloud locally and cost-effectively in places where connecting to the internet might not be an option. AWS Snowball is a perfect choice if you need to run computing in rugged, austere, mobile, or disconnected (or intermittently connected) environments.

With AWS Snowball, you have the choice of two devices, **Snowball Edge Compute Optimized** with more computing capabilities, suited for higher performance workloads, or **Snowball Edge Storage Optimized** with more storage, which is suited for large-scale data migrations and capacity-oriented workloads.

Snowball Edge Storage Optimized is the optimal choice if you need to securely and quickly transfer dozens of terabytes to petabytes of data to AWS. It is also a good fit for running general purpose analysis such as IoT data aggregation and transformation.

Snowball Edge Compute Optimized is the optimal choice if you need powerful compute and high-speed storage for data processing. Examples include high-resolution video processing, advanced IoT data analytics, and real-time optimization of machine learning models.

The other options are incorrect:

"A catalog of third-party software solutions that customers need to build solutions and run their businesses" is incorrect. AWS Marketplace is the service that provides this catalog. AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. AWS Marketplace includes software listings from categories such as security, networking, storage, machine learning, business intelligence, database, and DevOps.

"A hybrid cloud storage between on-premises environments and the AWS Cloud" is incorrect. AWS Storage Gateway is the service that enables your on-premises applications to seamlessly use AWS cloud storage.

"An Exabyte-scale data transfer service that allows you to move extremely large amounts of data to AWS" is incorrect. AWS Snowmobile is the exabyte-scale data migration service that allows you to move very large datasets from on-premises to AWS.

References:

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

Question 5:

Skipped

Which of the following are examples of AWS-Managed Services, where AWS is responsible for the operational and maintenance burdens of running the service? (Choose TWO)

- **Amazon Elastic Compute Cloud**
- **Amazon VPC**
- **Amazon DynamoDB**

  (Correct)

- **Amazon Elastic MapReduce**

  (Correct)

- **AWS IAM**

Explanation

For managed services such as Amazon Elastic MapReduce (Amazon EMR) and DynamoDB, AWS is responsible for performing all the operations needed to keep the service running.

Amazon EMR launches clusters in minutes. You don't need to worry about node provisioning, infrastructure setup, Hadoop configuration, or cluster tuning. Amazon EMR takes care of these tasks so you can focus on analysis.

DynamoDB is serverless with no servers to provision, patch, or manage and no software to install, maintain, or operate. DynamoDB automatically scales tables up and down to adjust for capacity and maintain performance. Availability and fault tolerance are built in, eliminating the need to architect your applications for these capabilities.

Other managed services include: AWS Lambda, Amazon RDS, Amazon Redshift, Amazon CloudFront, Amazon S3 and several other services.

For these managed services, AWS is responsible for most of the configuration and management tasks, but customers are still responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

NOTE:

The AWS managed services we mentioned above are different than the AWS Managed Services (AMS) service. AMS is an AWS service that operates AWS on behalf of enterprise customers and partners. Enterprises want to adopt AWS at scale but often the skills that have served them well in traditional IT do not always translate to success in the cloud. AWS Managed Services (AMS) enables them to migrate to AWS at scale more quickly, reduce their operating costs, improve security and compliance and focus on their differentiating business priorities.

The other options are incorrect:

"Amazon VPC" is incorrect. Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment. Amazon VPC is not a managed service, you are responsible for managing almost everything when using the Amazon VPC service.

"Amazon Elastic Compute Cloud" is incorrect. Amazon Elastic Compute Cloud (Amazon EC2) is a service that gives you complete control over your compute resources. Apart from patching the underlying host - which is the responsibility of AWS - you are responsible for managing almost everything in your server instances when using Amazon EC2.

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

References:

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

https://aws.amazon.com/emr/

Question 6:

Skipped

Which of the following does NOT belong to the AWS Cloud Computing models?

- **Networking as a Service (NaaS)**

  (Correct)

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**

Explanation

There are three Cloud Computing Models:

1) Infrastructure as a Service (IaaS) - Infrastructure as a Service (IaaS) contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS 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.

2) Platform as a Service (PaaS) - Platform as a Service (PaaS) removes the need for your organization to manage the underlying infrastructure (usually hardware and operating systems) and allows 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.

3) Software as a Service (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 of software. A common example of a SaaS application is web-based email which you can use to send and receive email without having to manage feature additions to the email product or maintain the servers and operating systems that the email program is running on.

Networking services are provided as part of the IaaS model.

References:

https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/types-of-cloud-computing.html

Question 7:

Skipped

Which of the below is a best-practice when designing solutions on AWS?

- **Use AWS reservations to reduce costs when testing your production environment**
- **Invest heavily in architecting your environment, as it is not easy to change your design later**
- **Automate wherever possible to make architectural experimentation easier**

  (Correct)

- **Provision a large compute capacity to handle any spikes in load**

Explanation

The Well-Architected Framework identifies a set of general design principles to facilitate good design in the cloud:

1- Stop guessing your capacity needs: Eliminate guessing about your infrastructure capacity needs. When you make a capacity decision before you deploy a system, you might end up sitting on expensive idle resources or dealing with the performance implications of limited capacity. With cloud computing, these problems can go away. You can use as much or as little capacity as you need, and scale up and down automatically.

2- Test systems at production scale: In the cloud, you can create a production-scale test environment on demand, complete your testing, and then decommission the resources. Because you only pay for the test environment when it's running, you can simulate your live environment for a fraction of the cost of testing on premises.

3- Automate to make architectural experimentation easier: Automation allows you to create and replicate your systems at low cost and avoid the expense of manual effort. You can track changes to your automation, audit the impact, and revert to previous parameters when necessary.

4- Allow for evolutionary architectures: Allow for evolutionary architectures. In a traditional environment, architectural decisions are often implemented as static, one-time events, with a few major versions of a system during its lifetime. As a business and its context continue to change, these initial decisions might hinder the system's ability to deliver changing business requirements. In the cloud, the capability to automate and test on demand lowers the risk of impact from design changes. This allows systems to evolve over time so that businesses can take advantage of innovations as a standard practice.

5- Drive architectures using data: In the cloud you can collect data on how your architectural choices affect the behavior of your workload. This lets you make fact-based decisions on how to improve your workload. Your cloud infrastructure is code, so you can use that data to inform your architecture choices and improvements over time.

6- Improve through game days: Test how your architecture and processes perform by regularly scheduling game days to simulate events in production. This will help you understand where improvements can be made and can help develop organizational experience in dealing with events.

The other options are incorrect:

"Provision a large compute capacity to handle any spikes in load" is incorrect. Instead of provisioning a large compute capacity to handle the spikes in load, it is recommended to use the AWS Auto Scaling service to add or remove instances based on demand. The AWS Auto Scaling service allows you to automatically provision new resources to meet demand and maintain performance. When demand drops, AWS Auto Scaling will automatically remove any excess resource capacity, so you avoid overspending.

"Use AWS reservations to reduce costs when testing your production environment" is incorrect. Reservations in AWS are not an appropriate choice when you need to test your production environment, AWS reservations have a minimum term of one year.

"Invest heavily in architecting your environment, as it is not easy to change your design later" is incorrect. In AWS, you can test and provision your resources on-demand and pay only for what you use with no long-term contracts. This enables you to make any changes you want in your architecture design at any time without any risks.

References:

https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf page 4

Question 8:

Skipped

Which statement is true regarding the AWS Shared Responsibility Model?

- **Patching the guest OS is always the responsibility of AWS**
- **Responsibilities vary depending on the services used**

  (Correct)

- **Security of the IaaS services is the responsibility of AWS**
- **Security of the managed services is the responsibility of the customer**

Explanation

Customers should be aware that their responsibilities may vary depending on the AWS services chosen. For example, when using Amazon EC2, you are responsible for applying operating system and application security patches regularly. However, such patches are applied automatically when using Amazon RDS.

The other options are incorrect:

"Security of the IaaS services is the responsibility of AWS" is incorrect. AWS products that fall into the well-understood category of Infrastructure as a Service (IaaS) - such as Amazon EC2, and Amazon VPC - are completely under your control and require you to perform all of the necessary security configuration and management tasks. For example, for EC2 instances, you're responsible for management of the guest OS (including updates and security patches), any application software or utilities you install on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. These are basically the same security tasks that you're used to performing no matter where your servers are located.

"Security of the managed services is the responsibility of the customer" is incorrect. AWS is responsible for the security configuration of its managed services. Examples of these types of services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, and Amazon Elastic MapReduce. For most of these services, all you have to do is to configure logical access controls on the resources and protect your account credentials, but overall, the security configuration work is performed by the service.

"Patching the guest OS is always the responsibility of AWS" is incorrect.

A computer on which AWS runs one or more virtual machines is called a **host** machine, and each virtual machine is called a **guest** machine. AWS drives the concept of virtualization by allowing the physical host machine to operate multiple virtual machines as guests (for multiple customers) to help maximize the effective use of computing resources such as memory, network bandwidth and CPU cycles.

Patching the **guest** operating system is the responsibility of AWS for the managed services only (such as Amazon RDS). The customer is responsible for patching the guest OS for other services (such as Amazon EC2).

AWS is responsible for patching the underlying **hosts**, upgrading the firmware, and fixing flaws within the infrastructure for all services, including Amazon EC2.

References:

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

Question 9:

Skipped

What is the AWS service that provides a virtual network dedicated to your AWS account?

- **Amazon VPC**

(Correct)

- **AWS Dedicated Hosts**
- **AWS VPN**
- **AWS Subnets**

Explanation

Amazon Virtual Private Cloud (Amazon VPC) allows you to carve out a portion of the AWS Cloud that is dedicated to your AWS account. Amazon VPC enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

The other options are incorrect:

"AWS Dedicated Hosts" is incorrect. An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts can save you money by enabling you to leverage your existing server-bound software license investments (e.g., Windows Server, Windows SQL Server, and SUSE Linux Enterprise Server) within EC2, subject to your license terms. Dedicated Hosts also give you more flexibility, visibility, and control over the placement of instances on dedicated hardware. This makes it easier to ensure you deploy your instances in a way that meets your compliance and regulatory requirements.

"AWS VPN" is incorrect. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to AWS. AWS Client VPN enables you to securely connect users (from any location) to AWS or on-premises networks.

"AWS Subnets" is incorrect. A subnet is a range of IP addresses within a VPC.

References:

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

Question 10:

Skipped

A company has moved to AWS recently. Which of the following AWS Services will help ensure that they have the proper security settings? (Choose TWO)

- **Amazon CloudWatch**
- **Amazon SNS**
- **AWS Trusted Advisor**

(Correct)

- **Amazon Inspector**

(Correct)

- **Concierge Support Team**

Explanation

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of a detailed assessment report which is available via the Amazon Inspector console or API. To help get started quickly, Amazon Inspector includes a knowledge base of hundreds of rules mapped to common security best practices and vulnerability definitions. Examples of built-in rules include checking for remote root login being enabled, or vulnerable software versions installed. These rules are regularly updated by AWS security researchers.

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.** Like your customized cloud security expert, AWS Trusted Advisor analyzes your AWS environment and provides security recommendations to protect your AWS environment. The service improves the security of your applications by closing gaps, examining permissions, and enabling various AWS security features.

The other options are incorrect:

"Amazon SNS" is incorrect. Amazon SNS is a pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

"Concierge Support Team" is incorrect. The AWS Concierge Support Team is a specialized offering available only to customers having an Enterprise or Enterprise On-Ramp Support subscription. The Concierge Team assists customers with their billing and account inquiries.

"Amazon CloudWatch" is incorrect. Amazon CloudWatch is used to monitor the utilization of AWS resources and services. You can use CloudWatch to visualize system metrics, take automated actions, troubleshoot performance issues, discover insights to optimize your applications, and ensure they are running smoothly.

References:

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

https://aws.amazon.com/inspector/

Question 11:

Skipped

AWS allows users to manage their resources using a web based user interface. What is the name of this interface?

- **AWS SDK**
- **AWS CLI**
- **AWS Management Console**

  (Correct)

- **AWS API**

Explanation

The AWS Management Console allows you to access and manage Amazon Web Services through a simple and intuitive web-based user interface. You can also use the AWS Console mobile app to quickly view resources on the go.

The other options are incorrect:

AWS CLI is incorrect. The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

AWS SDK is incorrect. The AWS SDK (Software Development Kit) allows you to interact with AWS services using your preferred programming language.

AWS API is incorrect. AWS API refers to the AWS application programming interface.

References:

https://aws.amazon.com/console/

Question 12:

Skipped

Which of the following must an IAM user provide to interact with AWS services using the AWS Command Line Interface (AWS CLI)?

- **Secret token**
- **Access keys**

  (Correct)

- **User ID**
- **User name and password**

Explanation

Access keys consist of an access key ID and secret access key, which are used to sign programmatic requests to AWS using the CLI or the SDK.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

Question 13:

Skipped

Which of the below options are related to the reliability of AWS? (Choose TWO)

- **Providing compensation to customers if issues occur**
- **Automatically provisioning new resources to meet demand**

  (Correct)

- **Ability to recover quickly from failures**

  (Correct)

- **Applying the principle of least privilege to all AWS resources**
- **All AWS services are considered Global Services, and this design helps customers serve their international users**

Explanation

The reliability term encompasses 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. The automatic provisioning of resources and the ability to recover from failures meet these criteria.

The other options are incorrect:

"Applying the principle of least privilege to all AWS resources" is incorrect. Principle of least privilege is a security concept related to access management.

"Providing compensation to customers if issues occur" is incorrect. AWS generally does not provide compensation to customers if issues occur and doing so has nothing to do with reliability.

"All AWS services are considered Global Services, and this design helps customers serve their international users" is incorrect. AWS services are either Global, Regional or specific to an Availability Zone. Among all the services that AWS offers, only a few of them are considered global services. **Examples of AWS global services include: Amazon CloudFront, AWS Shield, AWS Identity and Access Management (AWS IAM) and Amazon Route 53.** This answer is incorrect because NOT ALL AWS Services are Global.

References:

https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/wellarchitected-reliability-pillar.pdf

Question 14:

Skipped

Your company has a data store application that requires access to a NoSQL database. Which AWS database offering would meet this requirement?

- **Amazon Elastic Block Store**
- **Amazon Aurora**
- **Amazon Redshift**
- **Amazon DynamoDB**

  (Correct)

Explanation

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity, makes it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

The other options are incorrect:

"Amazon Elastic Block Store" is incorrect. Amazon Elastic Block Store (Amazon EBS) is a storage service, NOT a database service.

"Amazon Aurora" is incorrect. Amazon Aurora doesn't support NoSQL databases. Amazon Aurora is a MySQL and PostgreSQL-compatible relational database.

"Amazon Redshift" is incorrect. Amazon Redshift doesn't support non-relational data. Amazon Redshift is a fully managed data warehouse service that allows you to run complex analytic queries against petabytes of structured data using standard SQL and your existing Business Intelligence (BI) tools.

References:

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

Question 15:

Skipped

As part of the Enterprise support plan, who is the primary point of contact for ongoing support needs?

- **AWS Identity and Access Management (IAM) user**
- **Infrastructure Event Management (IEM) engineer**
- **Technical Account Manager (TAM)**

  (Correct)

- **AWS Consulting Partners**

Explanation

For Enterprise-level customers, a TAM (Technical Account Manager) provides technical expertise for the full range of AWS services and obtains a detailed understanding of your use case and technology architecture. TAMs work with AWS Solution Architects to help you launch new projects and give best practices recommendations throughout the implementation life cycle. Your TAM is the primary point of contact for ongoing support needs, and you have a direct telephone line to your TAM.

The other options are incorrect:

"Infrastructure Event Management (IEM) engineer" is incorrect. AWS Infrastructure Event Management (IEM) is a structured program available to Enterprise Support customers (and Business Support customers for an additional fee) that helps you plan for **large-scale events** such as product or application launches, infrastructure migrations, and marketing events. With Infrastructure Event Management, you get strategic planning assistance before your event, as well as real-time support during these moments that matter most for your business. AWS Infrastructure Event Management is not for day-to-day support needs.

"AWS Identity and Access Management (IAM) user" is incorrect. An AWS Identity and Access Management (IAM) user is an entity that you create in AWS to represent the person or service that uses it to directly interact with AWS. A primary use for IAM users is to grant individuals access to the AWS Management Console for interactive tasks and / or to make programmatic requests to AWS services using the API or CLI.

"AWS Consulting Partners" is incorrect. AWS Consulting Partners are not part of AWS support. AWS Consulting Partners are professional services firms that help customers design, architect, build, migrate, and manage their workloads and applications on AWS. Consulting Partners include System Integrators, Strategic Consultancies, Agencies, Managed Service Providers, and Value-Added Resellers.

References:

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

Question 16:

Skipped

What does the "Principle of Least Privilege" refer to?

- **You should grant your users only the permissions they need when they need them and nothing more**

  (Correct)

- **All IAM users should have at least the necessary permissions to access the core AWS services**
- **IAM users should not be granted any permissions; to keep your account safe**

- **All trusted IAM users should have access to any AWS service in the respective AWS account**

Explanation

The principle of least privilege is one of the most important security practices and it means granting users the required permissions to perform the tasks entrusted to them and nothing more. The security administrator determines what tasks users need to perform and then attaches the policies that allow them to perform only those tasks. You should start with a minimum set of permissions and grant additional permissions when necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them down.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

Question 17:

Skipped

What does AWS provide to deploy popular technologies - such as IBM MQ - on AWS with the least amount of effort and time?

- **AWS Quick Start reference deployments**

  (Correct)

- **Amazon Aurora**
- **AWS OpsWorks**
- **Amazon CloudWatch**

Explanation

AWS Quick Start Reference Deployments outline the architectures for popular enterprise solutions on AWS and provide AWS CloudFormation templates to automate their deployment. Each Quick Start launches, configures, and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

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

The other options are incorrect:

AWS OpsWorks" is incorrect. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers.

"Amazon CloudWatch" is incorrect. Amazon CloudWatch is mainly used to monitor the utilization of your AWS resources.

"Amazon Aurora" is incorrect. Amazon Aurora is a database service.

References:

https://aws.amazon.com/quickstart/

Question 18:

Skipped

A company is introducing a new product to their customers, and is expecting a surge in traffic to their web application. As part of their Enterprise Support plan, which of the following provides the company with architectural and scaling guidance?

- **Infrastructure Event Management**

  (Correct)

- **AWS Support Concierge Service**
- **AWS Knowledge Center**
- **AWS Health Dashboard**

Explanation

AWS Infrastructure Event Management is a short-term engagement with AWS Support, included in the Enterprise-level Support product offering, and available for additional purchase for Business-level Support subscribers. AWS Infrastructure Event Management partners with your technical and project resources to gain a deep understanding of your use case and provide architectural and scaling guidance for an event. Common use-case examples for AWS Event Management include advertising launches, new product launches, and infrastructure migrations to AWS.

The other options are incorrect:

"AWS Health Dashboard" is incorrect. The AWS Health Dashboard (previously AWS Personal Health Dashboard) is the single place to learn about the availability and operations of AWS services. You can view the overall status of all AWS services, and you can sign in to access a personalized view of the health of the specific services that are powering your workloads and applications. AWS Health Dashboard proactively notifies you when AWS experiences any events that may affect you, helping provide quick visibility and guidance to minimize the impact of events in progress, and plan for any scheduled changes, such as AWS hardware maintenance.

AWS Knowledge Center is incorrect. AWS Knowledge Center is not part of the Enterprise support plan. AWS Knowledge Center is available for everyone free of charge. The AWS Knowledge Center helps answer the questions most frequently asked by AWS customers. The AWS Knowledge Center does not provide guidance on a case-by-case basis.

AWS Support Concierge Service is incorrect. AWS Support Concierge Service assists customers with account and billing inquiries.

References:

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

Question 19:

Skipped

What does Amazon CloudFront use to distribute content to global users with low latency?

- **AWS Edge Locations**

  (Correct)

- **AWS Availability Zones**
- **AWS Regions**
- **AWS Global Accelerator**

Explanation

To deliver content to global end users with lower latency, Amazon CloudFront uses a global network of Edge Locations and Regional Edge Caches in multiple cities around the world. Amazon CloudFront uses this network to cache copies of your content close to your end-users. Amazon CloudFront ensures that end-user requests are served by the closest edge location. As a result, end-user requests travel a short distance, improving performance for your end-users, while reducing the load on the origin servers.

The other options are incorrect:

AWS Global Accelerator is incorrect. AWS Global Accelerator and CloudFront are two separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable (e.g., images and videos) and dynamic content (e.g. dynamic site delivery). Global Accelerator is a good fit for specific use cases, such as gaming, IoT or Voice over IP.

"AWS Availability Zones" and "AWS Regions" are incorrect. Amazon CloudFront only uses Edge Locations or Regional Edge Caches.

References:

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

Question 20:

Skipped

You have noticed that several critical Amazon EC2 instances have been terminated. Which of the following AWS services would help you determine who took this action?

- **Amazon Inspector**
- **AWS Trusted Advisor**
- **EC2 Instance Usage Report**
- **AWS CloudTrail**

  (Correct)

Explanation

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

The other options are incorrect:

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

"EC2 Instance Usage Report" is incorrect. This report shows you your historical EC2 instance usage, and helps you plan for future EC2 usage. EC2 Instance Usage Reports are designed to make it easier for you to track and better manage your EC2 usage and spending.

"AWS Trusted Advisor" is incorrect. AWS Trusted Advisor is an online tool that provides real time guidance to help you provision your resources following AWS best practices.

References:

https://aws.amazon.com/cloudtrail/

Question 21:

Skipped

What is the advantage of the AWS-recommended practice of "decoupling" applications?

- **Allows treating an application as a single, cohesive unit**
- **Allows tracking of any API call made to any AWS service**
- **Allows updates of any monolithic application quickly and easily**
- **Reduces inter-dependencies so that failures do not impact other components of the application**

  (Correct)

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. On the other hand if the components of an application are tightly coupled and one component fails, the entire application will also fail. Therefore when designing your application, you should always decouple its components.

The other options are incorrect:

"Allows treating an application as a single, cohesive unit" is incorrect. Decoupling allows you to deal with your application as multiple independent components (microservices) not as a single, cohesive unit.

"Allows tracking of any API call made to any AWS service" is incorrect. There is no relation between decoupling an application and tracking API calls. API calls are tracked by AWS CloudTrail.

"Allows updates of any monolithic application quickly and easily" is incorrect. Decoupling is the exact opposite of having a monolithic application. A monolithic application is designed to be self-contained; components of the program are interconnected and interdependent rather than loosely coupled as is the case with Microservices applications (or loosely-coupled applications). Decoupling allows the update of any microservices application component to occur quickly and independently of the remainder of the application. This allows developers to work independently to update multiple components at the same time. On the other hand, a monolithic application is a single unit and takes more time and effort to be updated.

References:

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

Question 22:

Skipped

You have set up consolidated billing for several AWS accounts. One of the accounts has purchased a number of reserved instances for 3 years. Which of the following is true regarding this scenario?

- **There are no cost benefits from using consolidated billing; It is for informational purposes only**
- **The Reserved Instance discounts can only be shared with the master account**
- **The purchased instances will have better performance than On-demand instances**
- **All accounts can receive the hourly cost benefit of the Reserved Instances**

  (Correct)

Explanation

For billing purposes, the consolidated billing feature of AWS Organizations treats all the accounts in the organization as one account. This means that all accounts in the organization can receive the hourly cost benefit of Reserved

Instances that are purchased by any other account. For example, Suppose that Fiona and John each have an account in an organization. Fiona has five Reserved Instances of the same type, and John has none. During one particular hour, Fiona uses three instances and John uses six, for a total of nine instances on the organization's consolidated bill. AWS bills five instances as Reserved Instances, and the remaining four instances as On-demand instances.

The other options are incorrect:

"The purchased instances will have better performance than On-demand instances" is incorrect. There is no difference in performance between On-demand and Reserved instances of the same type.

"The Reserved Instance discounts can only be shared with the master account" is incorrect. The Reserved Instance discounts can be shared with all accounts in the organization.

"There are no cost benefits from using consolidated billing; It is for informational purposes only" is incorrect. With Consolidated Billing, you can combine the usage across all accounts in the organization to share the Reserved Instance discounts, volume pricing discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts.

References:

https://docs.aws.amazon.com/aws-technical-content/latest/cost-optimization-reservation-models/consolidated-billing.html

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

Question 23:

Skipped

A company has an AWS Enterprise Support plan. They want quick and efficient guidance with their billing and account inquiries. Which of the following should the company use?

- **AWS Support Concierge**

  (Correct)

- **AWS Health Dashboard**
- **AWS Customer Service**
- **AWS Operations Support**

Explanation

Included as part of the Enterprise Support plan, the Support Concierge Team are AWS billing and account experts that specialize in working with enterprise accounts. The Concierge team will quickly and efficiently assist you with your billing and account inquiries, and work with you to help implement billing and account best practices so that you can focus on running your business.

Support Concierge service includes:

** 24 x7 access to AWS billing and account inquires.

** Guidance and best practices for billing allocation, reporting, consolidation of accounts, and root-level account security.

** Access to Enterprise account specialists for payment inquiries, training on specific cost reporting, assistance with service limits, and facilitating bulk purchases.

The other options are incorrect:

"AWS Customer Service" is incorrect. AWS Customer Service can help AWS customers with their billing and account inquiries, and it is included in all AWS support plans (Basic, Developer, Business, and Enterprise). However, due to the fact that AWS Customer Service is not dedicated to specific types of inquiries, it is not as quick or as efficient as the AWS Support Concierge. AWS Support Concierge is available only for AWS Enterprise support subscribers and is dedicated only to help AWS customers with their billing and account inquiries.

"AWS Operations Support" is incorrect. AWS Operations Support is an Enterprise support program that provides operations assessments and analysis to identify gaps across the operations lifecycle, as well as recommendations based on best practices.

"AWS Health Dashboard" is incorrect. The AWS Health Dashboard (previously AWS Personal Health Dashboard) is the single place to learn about the availability and operations of AWS services. You can view the overall status of all AWS services, and you can sign in to access a personalized view of the health of the specific services that are powering your workloads and applications. AWS Health Dashboard proactively notifies you when AWS experiences any events that may affect you, helping provide quick visibility and guidance to minimize the impact of events in progress, and plan for any scheduled changes, such as AWS hardware maintenance.

References:

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

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

Question 24:

Skipped

Which service provides DNS in the AWS cloud?

- **Amazon EMR**
- **Amazon CloudFront**
- **Route 53**

  (Correct)

- **AWS Config**

Explanation

Amazon Route 53 is a global service that provides highly available and scalable Domain Name System (DNS) services, domain name registration, and health-checking web services. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications by translating names like example.com into the numeric IP addresses, such as 192.0.2.1, that computers use to connect to each other.

Route 53 also simplifies the hybrid cloud by providing recursive DNS for your Amazon VPC and on-premises networks over AWS Direct Connect or AWS VPN.

The other options are incorrect:

"Amazon EMR" is incorrect. EMR is used to process vast amounts of data easily and securely. Use cases include: big data,log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

"AWS Config" is incorrect. AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.

"Amazon CloudFront" is incorrect. Amazon CloudFront gives businesses and web application developers an easy and cost effective way to distribute content globally with low latency and high data transfer speeds.

References:

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

Question 25:

Skipped

What do you gain from setting up consolidated billing for five different AWS accounts under another master account?

- **Each AWS account gets five times the free-tier services capacity**
- **AWS services' costs will be reduced to half the original price**
- **Each AWS account gets volume discounts**

  (Correct)

- **The consolidated billing feature is just for organizational purposes**

Explanation

AWS consolidated billing enables an organization to consolidate payments for multiple AWS accounts within a single organization by making a single paying account. For billing purposes, AWS treats all the accounts on the consolidated bill as one account. Some services, such as Amazon EC2 and Amazon S3 have volume pricing tiers across certain usage dimensions that give the user lower prices when they use the service more. For example if you use 50 TB in each account you would normally be charged $23 *50*3 (because they are 3 different accounts), But with consolidated billing you would be charged $23*50+$22*50*2 (because they are treated as one account) which means that you would save $100.

HOW IT WORKS

After you create an organization and verify that you own the email address associated with the master (management) account, you can invite existing AWS accounts to join your organization. When you invite an account, the AWS Organizations service sends an invitation to the account owner, who decides whether to accept or decline the invitation. If they accept, their account becomes a member of that organization.

At the moment an account accepts the invitation to join an organization, the master account of the organization becomes liable for all charges accrued by the new member account. The payment method attached to the member account is no longer used. Instead, the payment method attached to the master account of the organization pays for all charges accrued by the member account.

References:

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

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_invites.html

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

Question 26:

Skipped

The principle “design for failure and nothing will fail” is very important when designing your AWS Cloud architecture. Which of the following would help adhere to this principle? (Choose TWO)

- **Availability Zones**

  (Correct)

- **Vertical Scaling**
- **Multi-factor authentication**
- **Elastic Load Balancing**

  (Correct)

- **Penetration testing**

Explanation

Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones. When designing your AWS Cloud architecture, you should make sure that your system will continue to run even if failures happen. You can achieve this by deploying your AWS resources in multiple Availability zones. Availability zones are isolated from each other; therefore, if one availability zone goes down, the other Availability Zones will still be up and running, and hence your application will be more fault-tolerant. In addition to availability zones, you can build a disaster recovery solution by deploying your AWS resources in other regions. If an entire region goes down, you will still have resources in another region able to continue to provide a solution. Finally, you can use the Elastic Load Balancing service to regularly perform health checks and distribute traffic only to healthy instances.

The other options are incorrect:

"Multi-factor authentication" is incorrect. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. Multi-Factor Authentication is much more related to security, not fault tolerance.

"Penetration testing" is incorrect. Penetration testing is the practice of testing a network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing is much more related to security, not fault tolerance.

"Vertical Scaling" is incorrect. A "vertically scalable" system is constrained to running its processes on only one computer; in such systems, the only way to increase performance is to add more resources into one computer in the form of faster (or more) CPUs, memory, or storage. Vertical scaling may improve performance, but not fault-tolerance; because if this "one computer" fails, the whole system will fail.

References:

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

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

Question 27:

Skipped

In the AWS Shared responsibility Model, which of the following are the responsibility of the customer? (Choose TWO)

- **Configuring network access rules**

  (Correct)

- **Disk disposal**
- **Patching the Network infrastructure**
- **Setting password complexity rules**

  (Correct)

- **Controlling physical access to compute resources**

Explanation

The customer is responsible for securing their network by configuring Security Groups, Network Access control Lists (Network ACLs), and Routing Tables. The customer is also responsible for setting a **password policy** on their AWS account that specifies the complexity and mandatory rotation periods for their IAM users' passwords.

The other options are incorrect:

"Disk disposal" is incorrect. Disk disposal (Storage Device Decommissioning): When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

"Controlling physical access to compute resources" is incorrect. AWS is responsible for controlling physical access to the data centers.

"Patching the Network infrastructure" is incorrect. Patching the underlying infrastructure is the responsibility of AWS. The customer is responsible for patching the Operating System of their EC2 instances and any software installed on these instances.

References:

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

Question 28:
Skipped
What is the AWS service that enables AWS architects to manage infrastructure as code?

- **Amazon SES**
- **AWS Config**
- **Amazon EMR**
- **AWS CloudFormation**

(Correct)

Explanation
AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. You create

a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. You don't need to individually create and configure AWS resources and figure out what's dependent on what; AWS CloudFormation handles all that for you.

The other options are incorrect:

"Amazon SES" is incorrect. Amazon SES refers to the Amazon Simple Email service.

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

"Amazon EMR" is incorrect. Amazon EMR is used to run and scale Apache Spark, Hadoop, Presto, and other Big Data Frameworks.

References:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html

Question 29:

Skipped

According to the AWS Acceptable Use Policy, which of the following statements is true regarding penetration testing of EC2 instances?

- **Penetration testing is not allowed in AWS**
- **Penetration testing can be performed by the customer on their own instances without prior authorization from AWS**

  (Correct)

- **The AWS customers are only allowed to perform penetration testing on services managed by AWS**
- **Penetration testing is performed automatically by AWS to determine vulnerabilities in your AWS infrastructure**

Explanation

AWS customers are welcome to carry out security assessments and penetration tests against their AWS infrastructure without prior approval for 8 services:

1- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers.

2- Amazon RDS.

3- Amazon CloudFront.

4- Amazon Aurora.

5- Amazon API Gateways.

6- AWS Lambda and Lambda Edge functions.

7- Amazon Lightsail resources.

8- Amazon Elastic Beanstalk environments.

The other options are incorrect.

"Penetration testing is performed automatically by AWS to determine vulnerabilities in your AWS infrastructure" is incorrect. The AWS customers are responsible for performing penetration tests against their AWS infrastructure.

"Penetration testing is not allowed in AWS" is incorrect. AWS customers are allowed to perform penetration tests against their AWS infrastructure, but they must ensure that their activities are aligned with AWS policies.

"The AWS customers are only allowed to perform penetration testing on services managed by AWS" is incorrect. AWS customers are allowed to perform penetration testing on both AWS-managed services such as Amazon RDS and customer-managed services such as Amazon EC2.

Additional information:

The difference between AWS-managed services and customer-managed services:

For AWS-managed services such as Amazon RDS and Amazon DynamoDB, AWS is responsible for performing all the operations needed to keep the service running.

The AWS-managed services automate time-consuming administration tasks such as hardware provisioning, software setup, patching and backups. The AWS-managed services free customers to focus on their applications so they can give them the fast performance, high availability, security and compatibility they need.

Examples of AWS-managed services include Amazon RDS, Amazon DynamoDB, Amazon Redshift, Amazon CloudFront, Amazon CloudSearch, and several other services.

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

Examples of customer-managed services include Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC), and AWS Identity And Access Management (AWS IAM).

References:

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

Question 30:

Skipped

Adjusting compute capacity dynamically to reduce cost is an implementation of which AWS cloud best practice?

- **Implement elasticity**

  (Correct)

- **Parallelize tasks**
- **Adopt monolithic architecture**
- **Build security in every layer**

Explanation

In the traditional data center-based model of IT, once infrastructure is deployed, it typically runs whether it is needed or not, and all the capacity is paid for, regardless of how much it gets used. In the cloud, resources are elastic, meaning they can instantly grow (to maintain performance) or shrink (to reduce costs).

The other options are incorrect.

"Adopt monolithic architecture" is incorrect. AWS recommends adopting microservices architecture, not monolithic architecture. With monolithic architectures, application components are **tightly coupled** and run as a single service. With a microservices architecture, an application is built as **loosely coupled** components.

Benefits of microservices architecture include:

1- Microservices allow each service to be independently scaled to meet demand for the application feature it supports.

2- Teams are empowered to work more independently and more quickly.

3- Microservices enable continuous integration and continuous delivery, making it easy to try out new ideas and to roll back if something doesn’t work.

4- Service independence increases an application’s resistance to failure. In a monolithic architecture, if a single component fails, it can cause the entire application to fail. With microservices, applications handle total service failure by degrading functionality and not crashing the entire application.

"Parallelize tasks" is incorrect. An example of parallelization is when you use a load balancer to distribute the incoming requests across multiple asynchronous instances or when you use the AWS multipart upload to upload large objects in parts. Adjusting capacity up or down based on demand defines the AWS Cloud elasticity not the parallelization.

"Build Security in every layer" is incorrect. This option is related to security.

References:

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

http://aws001.s3.amazonaws.com/trailhead/TrailHead_ArchitectingInTheCloud.pdf

Question 31:

Skipped

A company is deploying a new two-tier web application in AWS. Where should the most frequently accessed data be stored so that the application's response time is optimal?

- **Amazon EBS volume**
- **AWS OpsWorks**
- **Amazon ElastiCache**

  (Correct)

- **AWS Storage Gateway**

Explanation

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.

The primary purpose of an in-memory data store is to provide ultrafast (submillisecond latency) and inexpensive access to copies of data. Querying a database is always slower and more expensive than locating a copy of that data in a cache. Some database queries are especially expensive to perform. An example is queries that involve joins across multiple tables or queries with intensive calculations. By caching (storing) such query results, you pay the price of the query only once. Then you can quickly retrieve the data multiple times without having to re-execute the query.

The other options are incorrect:

"AWS Storage Gateway" is incorrect. AWS Storage Gateway is not a caching service, it is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage.

"Amazon EBS volume" is incorrect. An Amazon EBS volume is a durable, block-level storage device that you can attach to a single EC2 instance. You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application. You can also use them for throughput-intensive applications that perform continuous disk scans.

"AWS OpsWorks" is incorrect. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.

References:

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

Question 32:

Skipped

A developer is planning to build a two-tier web application that has a MySQL database layer. Which of the following AWS database services would provide automated backups for the application?

- **Amazon DynamoDB**
- **A MySQL database installed on an EC2 instance**
- **Amazon Aurora**

  (Correct)

- **Amazon Neptune**

Explanation

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud. Amazon Aurora combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. It delivers up to five times the throughput of standard MySQL and up to three times the throughput of standard PostgreSQL. Amazon Aurora is designed to be compatible with MySQL and with PostgreSQL, so that existing applications and tools can run without requiring modification. It is available through Amazon Relational Database Service (RDS), freeing you from time-consuming administrative tasks such as provisioning, patching, backup, recovery, failure detection, and repair.

The other options are incorrect:

"A MySQL database installed on an EC2 instance" is incorrect. You can Install MySQL on an EC2 instance, but in this scenario, you would have to manage the database and the backup processes yourself; it would not be automatic.

"Amazon DynamoDB" is incorrect. Amazon DynamoDB does not support MySQL. Amazon DynamoDB is a NoSQL database service.

"Amazon Neptune" is incorrect. Amazon Neptune is a graph database service, not a MySQL database service. Amazon Neptune is used to build and run applications that work with highly connected datasets, such as social networking, recommendation engines, and knowledge graphs.

References:

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

Question 33:

Skipped

One of the most important AWS best-practices to follow is the cloud architecture principle of elasticity. How does this principle improve your architecture's design?

- **By automatically provisioning the required AWS resources based on changes in demand**

  (Correct)

- **By reducing interdependencies between application components wherever possible**
- **By automatically scaling your AWS resources using an Elastic Load Balancer**
- **By automatically scaling your on-premises resources based on changes in demand**

Explanation

Before cloud computing, you had to overprovision infrastructure to ensure you had enough capacity to handle your business operations at the peak level of activity. Now, you can provision the amount of resources that you actually need, knowing you can instantly scale up or down with the needs of your business. This reduces costs and improves your ability to meet your users' demands.

The concept of Elasticity involves the ability of a service to scale its resources out or in (up or down) based on changes in demand. For example, Amazon EC2 Autoscaling can help automate the process of adding or removing Amazon EC2 instances as demand increases or decreases.

The other options are incorrect:

"By reducing interdependencies between application components wherever possible" is incorrect. Reducing interdependencies between application components is much more related to the concept of "Loose Coupling". Loose coupling is an approach that involves interconnecting the components in a system or network so that those components depend on each other to the least extent practical. Engineers should architect their system or application such that failure in one component does not negatively affect other components. Loosely coupled components make the system resilient and allow it to recover gracefully from failure.

"By automatically scaling your on-premises resources based on changes in demand" is incorrect. It is not possible to scale on-premises resources automatically. When deploying on-premises, you have to guess on your infrastructure capacity needs.

"By automatically scaling your AWS resources using an Elastic Load Balancer" is incorrect. Elastic Load Balancers do not scale resources. Elastic Load Balancers distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.

References:

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

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

Question 34:

Skipped

Which of the following is not a benefit of Amazon S3? (Choose TWO)

- **Amazon S3 provides 99.999999999% (11 9's) of data durability**
- **Amazon S3 can run any type of application or backend system**

  (Correct)

- **Amazon S3 can be scaled manually to store and retrieve any amount of data from anywhere**

  (Correct)

- **Amazon S3 stores any number of objects, but with object size limits**
- **Amazon S3 provides unlimited storage for any type of data**

Explanation

"Amazon S3 can run any type of application or backend system" is not a benefit of S3 and thus is a correct answer. Amazon S3 is a storage service not a compute service.

"Amazon S3 can be scaled manually to store and retrieve any amount of data from anywhere" is not a benefit of S3 and thus is a correct answer. Amazon S3 scales automatically to store and retrieve any amount of data from anywhere.

Companies today need the ability to simply and securely collect, store, and analyze their data at a massive scale. Amazon S3 is object storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices. It's a simple storage service that offers highly available, and infinitely scalable data storage infrastructure at very low costs. It is designed to deliver 99.999999999% durability, and stores data for millions of applications used by market leaders in every industry. S3 provides comprehensive security and compliance capabilities that meet even the most stringent regulatory requirements. It gives customers flexibility in the way they manage data for cost optimization, access control, and compliance. S3 provides query-in-place functionality, allowing you to run powerful analytics directly on your data at rest in S3. And Amazon S3 is the most supported cloud storage service available, with integration from the largest community of third-party solutions, systems integrator partners, and other AWS services.

Amazon S3 stores any number of objects, but each object does have a size limitation. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes.

References:

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

Question 35:

Skipped

Which service is used to ensure that messages between software components are not lost if one or more components fail?

- **Amazon SQS**

  (Correct)

- **Amazon Connect**
- **Amazon SES**
- **AWS Direct Connect**

Explanation

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. SQS lets you decouple application components so that they run independently, increasing the overall fault tolerance of the system. Multiple copies of every message are stored redundantly across multiple availability zones so that they are available whenever needed.

The other options are incorrect:

Amazon SES is incorrect. Amazon SES (Amazon Simple Email Service) is a flexible, affordable, and highly-scalable email messaging platform for businesses and developers.

Amazon Connect is incorrect. Amazon Connect is a cloud-based contact center service that makes it easy for businesses to deliver customer service at low cost.

AWS Direct Connect is incorrect. AWS Direct Connect is a cloud service solution that is used to establish a dedicated network connection between your premises and AWS.

References:

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

Question 36:

Skipped

What is the AWS database service that allows you to upload data structured in key-value format?

- **Amazon Aurora**
- **Amazon DynamoDB**

  (Correct)

- **Amazon Redshift**
- **Amazon RDS**

Explanation

Amazon DynamoDB is a NoSQL database service. NoSQL databases are used for non-structured data that are typically stored in JSON-like, key-value documents.

The other options are incorrect:

Amazon Redshift is incorrect. Amazon Redshift is a data warehouse service that only supports relational data, NOT key-value data.

Additional information:

Amazon Redshift is a fast, fully managed data warehouse service that is specifically designed for online analytic processing (OLAP) and business intelligence (BI) applications, which require complex queries against large datasets.

Amazon Aurora is incorrect. Amazon Aurora is a MySQL and PostgreSQL-compatible relational database NOT a key-value database.

Amazon RDS is incorrect. Amazon RDS is a relational database NOT a key-value database.

References:

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

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

Question 37:

Skipped

Which S3 storage class is best for data with unpredictable access patterns?

- **Amazon S3 Intelligent-Tiering**

  (Correct)

- **Amazon S3 Standard-Infrequent Access**
- **Amazon S3 Standard**
- **Amazon S3 Glacier Flexible Retrieval**

Explanation

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, Amazon S3 monitors access patterns of the objects in S3 Intelligent-Tiering, and moves the ones that have not been accessed for 30 consecutive days to the infrequent access tier. If an object in the infrequent access tier is accessed, it is automatically moved back to the frequent access tier. There are no retrieval fees when using the S3 Intelligent-Tiering storage class, and no additional tiering fees when objects are moved between access tiers. It is the ideal storage class for long-lived data with access patterns that are unknown or unpredictable.

The other options are incorrect:

"Amazon S3 Standard" is incorrect. S3 Standard offers high durability, availability, and performance object storage for frequently accessed data.

"Amazon S3 Standard-Infrequent Access" is incorrect. Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is for data that is accessed less frequently, but requires rapid access when needed.

"Amazon S3 Glacier Flexible Retrieval" is incorrect. Amazon S3 Glacier Flexible Retrieval (Formerly S3 Glacier) is a low-cost storage class for archive data that is accessed 1 - 2 times per year.

References:

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

Question 38:
Skipped
Which of the following is an example of horizontal scaling in the AWS Cloud?

- **Increasing the compute capacity of a single EC2 instance to address the growing demands of an application**
- **Adding more EC2 instances of the same size to handle an increase in traffic**

  (Correct)

- **Adding more RAM capacity to an EC2 instance**
- **Replacing an existing EC2 instance with a larger, more powerful one**

Explanation
Horizontal Scaling:

Scaling horizontally takes place through an increase in the number of resources (e.g., adding more hard drives to a storage array or adding more servers to support an application). This is a great way to build Internet-scale applications that leverage the elasticity of cloud computing.

Vertical Scaling:

Scaling vertically takes place through an increase in the specifications of an individual resource (e.g., upgrading a server with a larger hard drive, adding more memory, or provisioning a faster CPU). On Amazon EC2, this can easily be achieved by stopping an instance and resizing it to an instance type that has more RAM, CPU, I/O,or networking capabilities. This way of scaling can eventually hit a limit and it is not always a cost efficient or highly available approach. However, it is very easy to implement and can be sufficient for many use cases especially as a short term solution.

Additional information:

Vertical-scaling is often limited to the capacity constraints of a single machine, scaling beyond that capacity often involves downtime and comes with an upper limit. With horizontal-scaling it is often easier to scale dynamically by adding more machines in parallel. Hence, in most cases, horizontal-scaling is recommended over vertical-scaling.

The other options are incorrect:

All other options are examples of Vertical Scaling.

References:

https://wa.aws.amazon.com/wat.concept.horizontal-scaling.en.html

Question 39:

Skipped

A Japanese company hosts their applications on Amazon EC2 instances in the Tokyo Region. The company has opened new branches in the United States, and the US users are complaining of high latency. What can the company do to reduce latency for the users in the US while minimizing costs?

- **Deploying new Amazon EC2 instances in a Region located in the US**

  (Correct)

- **Registering a new US domain name to serve the users in the US**
- **Applying the Amazon Connect latency-based routing policy**

- **Building a new data center in the US and implementing a hybrid model**

Explanation

The only way to reduce latency for the US users is to provision new Amazon EC2 instances in a Region closer to or in the US, OR by using Amazon CloudFront to cache copies of the content in edge locations close to the US users. In both cases, user requests will travel a shorter distance over the network, and the performance will improve.

The other options are incorrect:

"Building a new data center in the US and implementing a hybrid model" is incorrect. Building a new data center in the US is significantly expensive.

"Applying the Amazon Connect latency-based routing policy" is incorrect. Latency-based routing is a feature of Amazon Route 53, not Amazon Connect. Amazon Connect is a cloud-based contact center service that helps businesses to deliver customer service at a low cost.

"Registering a new US domain name to serve the users in the US" is incorrect. There is no relation between domain names and latency. Domain names are global and not tied to a specific region.

A Domain name (example.com) is just a way to direct end-users to a specific website\application instead of using IP addresses (116.203.247.177, for example), which are very difficult to remember.

References:

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

Question 40:

Skipped

Under the shared responsibility model, which of the following is the responsibility of AWS?

- **Configuring infrastructure devices**

  (Correct)

- **Server-side encryption**
- **Filtering traffic with Security Groups**
- **Client-side encryption**

Explanation

Under the shared responsibility model, AWS is responsible for the hardware and software that run AWS services. This includes patching the infrastructure software and configuring infrastructure devices. As a customer, you are responsible for implementing best practices for data encryption, patching guest operating system and applications, identity and access management, and network & firewall configurations.

The other options are incorrect.

"Filtering traffic with Security Groups" is incorrect. The AWS Customer is responsible for all network and firewall configurations, including the configuration of Security Groups, Network Access Control Lists (Network ACLs), and Routing tables.

"Client-side encryption" and "Server-side encryption" are incorrect. According to the AWS Shared Responsibility Model, AWS Customers are responsible for Client-side encryption and Server-side encryption. However, for some AWS fully managed services such as Amazon DynamoDB, server-side encryption is automatically done by AWS. Amazon DynamoDB transparently encrypts and decrypts all tables when they are written to disk. There is no option to enable or disable Server-side encryption.

Additional information:

AWS offers a lot of services and features that help AWS customers protect their data in the cloud. Customers can protect their data by encrypting it in transit and at rest. They can use CloudTrail to log API and user activity, including who, what, and from where calls were made. They can also use the AWS Identity and Access Management (IAM) to control who can access or edit their data.

References:

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

Question 41:

Skipped

In order to implement best practices when dealing with a “Single Point of Failure,” you should attempt to build as much automation as possible in both detecting and reacting to failure. Which of the following AWS services would help? (Choose TWO)

- **Amazon Athena**
- **ECR**
- **ELB**

  (Correct)

- **Amazon EC2**
- **Auto Scaling**

  (Correct)

Explanation

You should attempt to build as much automation as possible in both detecting and reacting to failure. You can use services like ELB and Amazon Route53 to configure health checks and mask failure by only routing traffic to healthy endpoints. In addition, Auto Scaling can be configured to automatically replace unhealthy nodes. You can also replace unhealthy nodes using the Amazon EC2 auto-recovery feature or services such as AWS OpsWorks and AWS Elastic Beanstalk. It won’t be possible to predict every possible failure scenario on day one. Make sure you collect enough logs and metrics to understand normal system behavior. After you understand that, you will be able to set up alarms that trigger automated response or manual intervention.

The other options are incorrect:

ECR is incorrect. Amazon Elastic Container Registry (Amazon ECR) is a Docker container registry that allows developers to store, manage, and deploy Docker container images.

Amazon Athena is incorrect. Amazon Athena is an interactive query service that is mainly used to analyze data in Amazon S3 using standard SQL.

Amazon EC2 is incorrect. Amazon EC2 is a server-based compute service. Fault tolerance is not built-in, you have to architect for fault tolerance using the services we mentioned above.

Additional information:

Lambda is a serverless compute service. Serverless computing provides built-in fault tolerance. You don't need to architect for this capability since the service provides it by default.

References:

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

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

Question 42:

Skipped

You want to run a questionnaire application for only one day (without interruption), which Amazon EC2 purchase option should you use?

- **Dedicated instances**
- **On-demand instances**

  (Correct)

- **Spot instances**
- **Reserved instances**

Explanation

With On-Demand instances, you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. 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:

"Reserved instances" is incorrect. Reserved instances are not appropriate in this case because the shortest reservation length is one year.

"Spot instances" is incorrect. Spot instances is not the right choice because the application must run without interruption.

"Dedicated instances" is incorrect. Dedicated instances can be used if you require your instance be physically isolated at the host hardware level from instances that belong to other AWS accounts.

References:

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

Question 43:

Skipped

You have deployed your application on multiple Amazon EC2 instances. Your customers complain that sometimes they can't reach your application. Which AWS service allows you to monitor the performance of your EC2 instances to assist in troubleshooting these issues?

- **AWS Lambda**
- **AWS Config**
- **AWS CloudTrail**
- **Amazon CloudWatch**

  (Correct)

Explanation

Amazon CloudWatch is a service that monitors AWS cloud resources and the applications you run 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. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use CloudWatch to detect anomalous behavior in your environments, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly.

The other options are incorrect:

"AWS Config" is incorrect. AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time. These capabilities enable compliance auditing, security analysis, and resource change tracking.

"AWS CloudTrail" is incorrect. AWS CloudTrail is an AWS service that can be used to monitor all user interactions with the AWS environment.

"AWS Lambda" is incorrect. AWS Lambda is a serverless compute service.

References:

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

Question 44:

Skipped

A startup company is operating on limited funds and is extremely concerned about cost overruns. Which of the below options can be used to notify the company when their monthly AWS bill exceeds $2000? (Choose TWO)

- **Configure the Amazon Connect Service to alert the company when the threshold is exceeded**
- **Configure the AWS Budgets Service to alert the company when the threshold is exceeded**

  (Correct)

- **Setup a CloudWatch billing alarm that triggers an SNS notification when the threshold is exceeded**

  (Correct)

- **Configure AWS CloudTrail to automatically delete all AWS resources when the threshold is exceeded**
- **Configure the Amazon Simple Email Service to send billing alerts to their email address on a daily basis**

Explanation

In CloudWatch, you can set up a billing alarm that triggers if your costs exceed a threshold that you set. This CloudWatch alarm can also be configured to trigger an SNS notification to your email address.

AWS Budgets is another AWS service that can be used in this scenario. 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. The difference between AWS Budgets and Amazon CloudWatch billing alarms is that Amazon CloudWatch billing alarms alert you only when your **actual** cost exceeds a certain threshold, while AWS Budgets can be configured to alert you when the **actual** or **forecasted** cost exceeds a certain threshold.

The other options are incorrect:

"Configure the Amazon Connect Service to alert the company when the threshold is exceeded" is incorrect. Amazon Connect is a self-service, cloud-based contact center service that makes it easy for any business to deliver better customer service at lower cost. Amazon Connect cannot be used to send billing notifications.

"Configure the Amazon Simple Email Service to send billing alerts to their email address on a daily basis" is incorrect. Amazon Simple Email Service (Amazon SES) is a cloud-based email sending service designed to help digital marketers and application developers send marketing, notification, and transactional emails. Amazon SES cannot be used to send billing alerts.

"Configure AWS CloudTrail to automatically delete all AWS resources when the threshold is exceeded" is incorrect. AWS customers setup billing alarms to manage and adjust their budgets, not to delete all AWS resources. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing by logging all API calls made within your AWS account. AWS CloudTrail cannot be used to delete AWS resources.

References:

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

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

Question 45:

Skipped

What should you do in order to keep the data on EBS volumes safe? (Choose TWO)

- **Prevent any unauthorized access to AWS data centers**
- **Ensure that EBS data is encrypted at rest**

  (Correct)

- **Store a backup daily in an external drive**
- **Regularly update firmware on EBS devices**
- **Create EBS snapshots**

  (Correct)

Explanation

Creating snapshots of EBS Volumes can help ensure that you have a backup of your EBS volumes just in case any issues arise. You can use **Amazon Data Lifecycle Manager (Amazon DLM)** to automate the **creation, retention, and deletion** of EBS snapshots.

Automating snapshot management with Amazon DLM helps you to:

- Protect valuable data by enforcing a regular backup schedule.

- Retain backups as required by auditors or internal compliance.

- Reduce storage costs by deleting outdated backups.

- Create disaster recovery backup policies that back up data to isolated accounts.

Amazon EBS encryption offers a straight-forward encryption solution for your EBS resources that doesn't require you to build, maintain, and secure your own key management infrastructure. Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

The other options are incorrect:

"Prevent any unauthorized access to AWS data centers" is incorrect. It is the responsibility of AWS to control and restrict access to its data centers.

"Store a backup daily in an external drive" is incorrect. To make a backup of your EBS volumes you should use the Snapshot feature. Snapshots can provide a Copy-on-Write Consistency (reflect the exact image of the volume at the point-in-time of the snapshot).

"Regularly update firmware on EBS devices" is incorrect. It is the responsibility of AWS to regularly update firmware on hardware devices.

Additional information:

EBS Snapshots are incremental backups, which means that only the blocks on the device that have changed after your last snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data.

References:

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

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

Question 46:

Skipped

Which service provides object-level storage in AWS?

- **Amazon EFS**
- **Amazon S3**

  (Correct)

- **Amazon Instance Store**
- **Amazon EBS**

Explanation

Amazon S3 is an object level storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices. It is designed to deliver 99.999999999% durability, and stores data for millions of applications used by market leaders in every industry.

The other options are incorrect:

"Amazon EFS" is incorrect. Amazon EFS is a **file-level** storage technology that provides massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistently low latencies.

"Amazon EBS" is incorrect. Amazon EBS is a **block-level** storage that provides storage volumes for use with Amazon EC2 and Amazon RDS instances.

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

References:

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

https://aws.amazon.com/what-is-cloud-object-storage/

Question 47:

Skipped

Your company is developing a critical web application in AWS, and the security of the application is a top priority. Which of the following AWS services will provide infrastructure security optimization recommendations?

- **AWS Trusted Advisor**

  (Correct)

- **AWS Secrets Manager**
- **AWS Shield**
- **AWS Management Console**

Explanation

AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices. 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 (also referred to as service quotas).

AWS Trusted Advisor improves the security of your application by closing gaps, enabling various AWS security features, and examining your permissions.

The core security checks include: (Important)

1- Security Groups - Specific Ports Unrestricted.

Checks security groups for rules that allow unrestricted access to specific ports. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

2- Amazon S3 Bucket Permissions.

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions. Bucket permissions that grant List access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access to everyone create potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket. This check examines explicit bucket permissions and associated bucket policies that might override the bucket permissions.

3- MFA on Root Account.

Checks the root account and warns if multi-factor authentication (MFA) is not enabled. For increased security, AWS recommends that you protect your account by using MFA, which requires a user to enter a unique authentication code from their MFA hardware or virtual device when interacting with the AWS console and associated websites.

The other options are incorrect:

"AWS Shield" is incorrect. AWS Shield does not provide security recommendations. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

"AWS Management Console" is incorrect. The AWS Management Console is used to access and manage Amazon Web Services through a simple and intuitive web-based user interface. The console itself doesn’t provide any recommendations.

"AWS Secrets Manager" is incorrect. AWS Secrets Manager does not provide security recommendations. AWS Secrets Manager is a secrets management service that enables you to store, retrieve, rotate, audit, and monitor secrets centrally. AWS Secrets Manager allows you to manage secrets such as database credentials, on-premises resource credentials, SaaS application credentials, third-party API keys, and Secure Shell (SSH) keys.

References:

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

Question 48:

Skipped

Which of the following is **NOT** correct regarding Amazon EC2 On-demand instances?

- **With on-demand instances, no longer-term commitments or upfront payments are needed**
- **The on-demand instances follow the AWS pay-as-you-go pricing model**

- **You have to pay a start-up fee when launching a new instance for the first time**

  (Correct)

- **When using on-demand Linux instances, you are charged per second based on an hourly rate**

Explanation
There are no startup or termination fees associated with Amazon EC2.

The other options are incorrect:

"The on-demand instances follow the AWS pay-as-you-go pricing model" is incorrect. AWS pay-as-you-go pricing model is similar to how you pay for utilities like water and electricity. With Amazon EC2 *on-demand instances,* you only pay for the compute capacity you consume, and once you stop using them, there are no additional costs or termination fees.

"With on-demand instances, no longer-term commitments or upfront payments are needed" is incorrect. 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.

"When using on-demand Linux instances, you are charged per second based on an hourly rate" is incorrect. With per-second billing, you pay for only what you use. It takes cost of unused minutes and seconds in an hour off of the bill, so you can focus on improving your applications instead of maximizing usage to the hour. Especially, if you manage instances running for irregular periods of time, such as dev/testing, data processing, analytics, batch processing and gaming applications, can benefit.

Per-second billing is available for instances launched in:

- On-Demand, Reserved and Spot forms

- All regions and Availability Zones

- Amazon Linux, Windows and Ubuntu

References:

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

Question 49:

Skipped

A global company with a large number of AWS accounts is seeking a way in which they can centrally manage billing and security policies across all accounts. Which AWS Service will assist them in meeting these goals?

- **AWS Trusted Advisor**
- **IAM User Groups**
- **AWS Config**
- **AWS Organizations**

  (Correct)

Explanation

AWS Organizations helps customers centrally govern their environments as they grow and scale their workloads on AWS. Whether customers are a growing startup or a large enterprise, Organizations helps them to centrally manage billing; control access, compliance, and security; and share resources across their AWS accounts.

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.

The other options are incorrect:

"AWS Trusted Advisor" is incorrect. AWS Trusted Advisor is an online tool that provides customers with real time guidance to help them provision their resources following AWS best practices.

"IAM User Groups" is incorrect. IAM user groups are not used to manage multiple AWS accounts. An IAM user group is a collection of IAM users - within the same AWS account - that are managed as a unit. IAM user groups let customers specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, customers could have a user group called Admins and give that user group the types of permissions that administrators typically need.

"AWS Config" is incorrect. AWS Config is a fully managed service that provides customers with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.

References:

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

Question 50:

Skipped

A company has decided to migrate its Oracle database to AWS. Which AWS service can help achieve this without negatively impacting the functionality of the source database?

- **AWS Server Migration Service**
- **AWS OpsWorks**
- **AWS Database Migration Service**

  (Correct)

- **AWS Application Discovery Service**

Explanation

AWS Database Migration Service (DMS) helps you migrate databases to AWS easily and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from most widely used commercial and open-source databases. The service supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora or Microsoft SQL Server to MySQL. It also allows you to stream data to Amazon Redshift from any of the supported sources including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, SAP ASE, and SQL Server, enabling consolidation and easy analysis of data in the petabyte-scale data warehouse. AWS Database Migration Service can also be used for continuous data replication with high availability.

The other options are incorrect:

"AWS OpsWorks" is incorrect. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.

"AWS Server Migration Service" is incorrect. AWS Server Migration Service (SMS) is used to migrate your on-premises workloads to AWS.

"AWS Application Discovery Service" is incorrect. AWS Application Discovery Service helps enterprise customers plan migration projects by gathering information about their on-premises data centers.

References:

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

Question 51:

Skipped

Which of the following services allows customers to manage their agreements with AWS?

- **AWS Organizations**
- **AWS Systems Manager**
- **AWS Certificate Manager**
- **AWS Artifact**

  (Correct)

Explanation

AWS Artifact is a self-service audit artifact retrieval portal that provides customers with on-demand access to AWS' compliance documentation and AWS agreements. You can use AWS Artifact Agreements to review, accept, and track the status of AWS agreements such as the Business Associate Addendum (BAA).

Additional information:

You can also use AWS Artifact Reports to download AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and System and Organization Control (SOC) reports.

The other options are incorrect:

"AWS Organizations" is incorrect. AWS Organizations provides central governance and management across multiple AWS accounts.

"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.

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

References:

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

Question 52:

Skipped

A company is planning to host an educational website on AWS. Their video courses will be streamed all around the world. Which of the following AWS services will help achieve high transfer speeds?

- **Amazon Kinesis Video Streams**
- **Amazon CloudFront**

  (Correct)

- **AWS CloudFormation**
- **Amazon SNS**

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, high transfer speeds, all within a developer-friendly environment.

The use cases of Amazon CloudFront include:

1- Accelerate static website content delivery.

CloudFront can speed up the delivery of your static content (for example, images, style sheets, JavaScript, and so on) to viewers across the globe. By using CloudFront, you can take advantage of the AWS backbone network and CloudFront edge servers to give your viewers a fast, safe, and reliable experience when they visit your website.

2- Live & on-demand video streaming.
The Amazon CloudFront CDN offers multiple options for streaming your media – both pre-recorded files and live events – at sustained, high throughput required for 4K delivery to global viewers.

3- Security.

CloudFront integrates seamlessly with AWS Shield for Layer 3/4 DDoS mitigation and AWS WAF for Layer 7 protection.

4- Customizable content delivery with Lambda@Edge.

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

The other options are incorrect:

"AWS CloudFormation" is incorrect. AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.

"Amazon Kinesis Video Streams" is incorrect. Amazon Kinesis Video Streams enables you to securely stream video from connected devices (IoT devices) to AWS for analytics, machine learning (ML), playback, and other processing. Kinesis Video Streams automatically provisions and elastically scales all the infrastructure needed to ingest streaming video data from millions of devices. It durably stores, encrypts, and indexes video data in your streams, and allows you to access your data through easy-to-use APIs.

"Amazon SNS" is incorrect. Amazon Simple Notification Service (SNS) is a fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Using Amazon SNS topics, your publisher systems can fan out messages to a large number of subscriber endpoints for parallel processing, including AWS Lambda functions, and HTTP/S webhooks. Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

References:

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

Question 53:

Skipped

You work as an on-premises MySQL DBA. The work of database configuration, backups, patching, and DR can be time-consuming and repetitive. Your company has decided to migrate to the AWS Cloud. Which of the following can help save time on database maintenance so you can focus on data architecture and performance?

- **Amazon Redshift**
- **Amazon RDS**

  (Correct)

- **Amazon CloudWatch**
- **Amazon DynamoDB**

Explanation

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity while automating time-consuming administration tasks such as hardware provisioning, operating system maintenance, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

Amazon RDS can be used to host Amazon Aurora, PostgreSQL, **MySQL**, MariaDB, Oracle, and Microsoft SQL Server databases.

The other options are incorrect:

"Amazon Redshift" is incorrect. Amazon Redshift is not a MySQL database service. Amazon Redshift is a fully managed data warehouse service that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools.

"Amazon DynamoDB" is incorrect. Amazon DynamoDB is not a MySQL database service. Amazon DynamoDB is a fully managed NoSQL database service.

"Amazon CloudWatch" is incorrect. Amazon CloudWatch is not a database service. Amazon CloudWatch is a monitoring service that gives you complete visibility of your cloud resources and applications

References:

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

Question 54:

Skipped

Hundreds of thousands of DDoS attacks are recorded every month worldwide. What service does AWS provide to help protect AWS Customers from these attacks? (Choose TWO)

- **AWS KMS**
- **Amazon Cognito**
- **AWS Config**
- **AWS Shield**

  (Correct)

- **AWS WAF**

  (Correct)

Explanation

AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures that follow AWS Best Practices for DDoS Resiliency. These include services such as **Amazon Route 53, Amazon CloudFront, Elastic Load Balancing, and AWS WAF** to control and absorb traffic, and deflect unwanted requests. These services integrate with **AWS Shield**, a managed DDoS protection service that provides always-on detection and automatic inline mitigations to safeguard web applications running on AWS.

The other options are incorrect:

"Amazon Cognito" is incorrect. Amazon Cognito allows you to add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

"AWS KMS" is incorrect. AWS KMS provides a highly available key storage, management, and auditing solution for you to encrypt data within your own applications and control the encryption of stored data across AWS services.

"AWS Config" is incorrect. AWS Config is a service that enables you to monitor, assess, and audit all changes made to your AWS resources.

References:

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

Question 55:

Skipped

Which of the following can be described as a global content delivery network (CDN) service?

- **AWS Direct Connect**
- **AWS VPN**
- **AWS Regions**
- **Amazon CloudFront**

  (Correct)

Explanation

Amazon CloudFront is a global content delivery network (CDN) service that gives businesses and web application developers an easy and cost effective way to distribute content (such as videos, data, applications, and APIs) with low latency and high data transfer speeds. Like other AWS services, Amazon CloudFront is a self-service, pay-per-use offering, requiring no long term commitments or minimum fees. With CloudFront, your files are delivered to end-users using a global network of edge locations. CloudFront is integrated with other AWS services such as AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code close to your viewers.

The other options are incorrect:

"AWS Direct Connect" is incorrect. AWS Direct Connect allows you to establish a dedicated network connection from your premises to AWS.

"AWS Regions" is incorrect. An AWS Region is a physical location in the world where AWS have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

"AWS VPN" is incorrect. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to AWS. AWS Client VPN enables you to securely connect users (from any location) to AWS or on-premises networks.

References:

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

Question 56:

Skipped

The identification process of an online financial services company requires that new users must complete an online interview with their security team. The completed recorded interviews are only required in the event of a legal issue or a regulatory compliance breach. What is the most cost-effective service to store the recorded videos?

- **Amazon S3 Glacier Deep Archive**

  (Correct)

- **AWS Marketplace**
- **S3 Intelligent-Tiering**
- **Amazon EBS**

Explanation

Amazon S3 Glacier Deep Archive is an extremely low-cost storage service that provides secure, durable, and flexible storage for long-term data backup and archival. With Amazon S3 Glacier Deep Archive, customers can reliably store their data for as little as $1 per terabyte per month, a significant savings compared to on-premises solutions. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so that they don’t have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and repair, or time-consuming hardware migrations.

The other options are incorrect:

"S3 Intelligent-Tiering" is incorrect. S3 Intelligent-Tiering is ideal for data with unknown or changing access patterns.

S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers - frequent access and infrequent access - when access patterns change.

"AWS Marketplace" is incorrect. 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. AWS Marketplace includes thousands of software listings from popular categories such as security, networking, storage, machine learning, business intelligence, database, and DevOps. 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, and get billed from one source, AWS.

"Amazon EBS" is incorrect. Amazon EBS is a block level storage that provides storage volumes for use with Amazon EC2 and Amazon RDS. Amazon EBS is not a cost-effective choice here.

References:

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

Question 57:

Skipped

An organization has decided to purchase an Amazon EC2 Reserved Instance (RI) for three years in order to reduce costs. It is possible that the application workloads could change during the reservation period.

What is the EC2 Reserved Instance (RI) type that will allow the company to exchange the purchased reserved instance for another reserved instance with higher computing power if they need to?

- **Standard RI**
- **Premium RI**
- **Convertible RI**

  (Correct)

- **Elastic RI**

Explanation

When your needs change, you can exchange your Convertible Reserved Instances and continue to benefit from the reservation's pricing discount. With Convertible RIs, you can exchange one or more Reserved Instances for another Reserved Instance with a different configuration, including **instance family, operating system, and tenancy.** There are no limits to how many times you perform an exchange, as long as the new Convertible Reserved Instance is of an equal or higher value than the original Convertible Reserved Instances that you are exchanging.

The other options are incorrect:

"Standard RIs" is incorrect. You cannot **exchange** Standard Reserved Instances, but you can **modify** them. You can modify attributes such as the Availability Zone, instance size (**within the same instance family**), and scope of your Reserved Instance (regional or zonal). Standard RIs provide the most significant discount (up to 72% off On-Demand) and are best suited for steady-state usage.

"Elastic RIs" and "Premium RIs" are not valid RI types.

References:

https://aws.amazon.com/ec2/pricing/reserved-instances/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-convertible-exchange.html

Question 58:

Skipped

You are working on a project that involves creating thumbnails of millions of images. Consistent uptime is not an issue, and continuous processing is not required. Which EC2 buying option would be the most cost-effective?

- **On-demand Instances**
- **Reserved Instances**
- **Spot Instances**

  (Correct)

- **Dedicated Instances**

Explanation

Spot instances provide a discount (up to 90%) off the On-Demand price. The Spot price is determined by long-term trends in supply and demand for EC2 spare capacity. If the Spot price exceeds the maximum price you specify for a given instance or if capacity is no longer available, your instance will automatically be interrupted.

Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if you don't mind if your applications get interrupted. For example, Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks.

The other options are incorrect:

"Reserved instances" is incorrect. Reserved instances are recommended for Customers who can commit to using EC2 over a 1 or 3-year term to reduce their total computing costs. Even if the project will last for more than a year, the cost-benefit for acquiring Reserved Instances is not as great as the cost-benefit from using Spot Instances. The Spot option provides the largest discount (up to 90%).

"On-demand instances" is incorrect. On-demand instances are significantly less cost-effective than spot instances.

"Dedicated instances" is incorrect. Dedicated instances are used when you need your instances to be physically isolated at the host hardware level from instances that belong to other AWS accounts. Dedicated instances are significantly more expensive than Spot Instances

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html

Question 59:

Skipped

Select TWO examples of the AWS shared controls.

- **Data Center operations**
- **Patch Management**

  (Correct)

- **Configuration Management**

  (Correct)

- **IAM Management**
- **VPC Management**

Explanation

Shared Controls are controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services.

Examples include:

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

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

** Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

Additional information:

A computer on which AWS runs one or more virtual machines is called a **host** machine, and each virtual machine is called a **guest** machine. AWS drives the concept of virtualization by allowing the physical host machine to operate multiple virtual machines as guests (for multiple customers) to help maximize the effective use of computing resources such as memory, network bandwidth and CPU cycles.

The other options are incorrect:

"Data Center operations" is incorrect. Data Center operations are an AWS responsibility.

"VPC Management" and "IAM Management" are incorrect. VPC and IAM management are customer responsibilities.

References:

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

Question 60:

Skipped

A company has developed an eCommerce web application in AWS. What should they do to ensure that the application has the highest level of availability?

- **Deploy the application across multiple Availability Zones and Edge locations**
- **Deploy the application across multiple VPC's and subnets**
- **Deploy the application across multiple Regions and Availability Zones**

  (Correct)

- **Deploy the application across multiple Availability Zones and subnets**

Explanation

The AWS Global infrastructure is built around Regions and Availability Zones (AZs). Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones. Availability Zones in a region are connected with low latency, high throughput, and highly redundant networking. These Availability Zones offer AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures.

In addition to replicating applications and data across multiple data centers in the same Region using Availability Zones, you can also choose to increase redundancy and fault tolerance further by replicating data between geographic Regions (especially if you are serving customers from all over the world). You can do so using both private, high speed networking and public internet connections to provide an additional layer of business continuity, or to provide low latency access across the globe.

The other options are incorrect:

"Deploy the application across multiple Availability Zones and subnets" is incorrect. A subnet is a range of IP addresses in your VPC.

"Deploy the application across multiple Availability Zones and Edge locations" is incorrect. Edge locations are not used to host applications. Edge locations are used by CloudFront to cache and distribute content to your global customers with low latency.

"Deploy the application across multiple VPC's and subnets" is incorrect. VPC refers to the virtual private cloud which is a virtual network that you define. Deploying the application across multiple VPC's within the same region will not help your global customers.

References:

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

Question 61:

Skipped

You have AWS Basic support, and you have discovered that some AWS resources are being used maliciously, and those resources could potentially compromise your data. What should you do?

- **Contact the AWS Concierge team**
- **Contact the AWS Customer Service team**
- **Contact the AWS Security team**
- **Contact the AWS Abuse team**

  (Correct)

Explanation

The AWS Abuse team can assist you when AWS resources are being used to engage in the following types of abusive behavior:

I. Spam: You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are being used to spam websites or forums.

II. Port scanning: Your logs show that one or more AWS-owned IP addresses are sending packets to multiple ports on your server, and you believe this is an attempt to discover unsecured ports.

III. Denial of service attacks (DOS): Your logs show that one or more AWS-owned IP addresses are being used to flood ports on your resources with packets, and you believe this is an attempt to overwhelm or crash your server or software running on your server.

IV. Intrusion attempts: Your logs show that one or more AWS-owned IP addresses are being used to attempt to log in to your resources.

V. Hosting objectionable or copyrighted content: You have evidence that AWS resources are being used to host or distribute illegal content or distribute copyrighted content without the consent of the copyright holder.

VI. Distributing malware: You have evidence that AWS resources are being used to distribute software that was knowingly created to compromise or cause harm to computers or machines on which it is installed.

Note: Anyone can report abuse of AWS resources, not just AWS customers.

The other options are incorrect:

"Contact the AWS Security team" is incorrect. The AWS Security team is responsible for the security of services offered by AWS.

"Contact the AWS Concierge team" is incorrect. The AWS Concierge team can assist you with the issues that are related to your billing and account management.

"Contact the AWS Customer Service team" is incorrect. The AWS Customer Service team is at the forefront of this transformational technology assisting a global list of customers that are taking advantage of a growing set of services and features to run their mission-critical applications. The team helps AWS customers understand what Cloud Computing is all about, and whether it can be useful for their business needs.

References:

https://aws.amazon.com/security/vulnerability-reporting/

Question 62:

Skipped

An organization has a large number of technical employees who operate their AWS Cloud infrastructure. What does AWS provide to help organize them into teams and then assign the appropriate permissions for each team?

- **AWS Organizations**
- **IAM user groups**

  (Correct)

- **IAM users**
- **IAM roles**

Explanation

An IAM user group is a collection of IAM users that are managed as a unit. User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, you could have a user group called Admins and give that user group the types of permissions that administrators typically need. Any user in that user group automatically has the permissions that are assigned to the user group. If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to that user group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old user groups and add him or her to the appropriate new user groups.

The other options are incorrect:

"IAM role" is incorrect. An IAM role is an IAM identity that you can create in your account that has specific permissions. IAM roles allow you to delegate access (for a limited time) to users or services that normally don't have access to your organization's AWS resources. IAM users or AWS services can assume a role to obtain temporary security credentials that can be used to interact with specific AWS resources.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app. Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources. For these scenarios, you can delegate access to AWS resources using an IAM role.

"IAM users" is incorrect. An IAM user is an entity that you create in AWS to represent the person or application that uses it to directly interact with AWS. A primary use for IAM users is to give people the ability to sign in to the AWS Management Console for interactive tasks and to make programmatic requests to AWS services using the API or CLI. A user in AWS consists of a name, a password to sign into the AWS Management Console, and up to two access keys that can be used with the API or CLI. When you create an IAM user, you grant it permissions by making it a member of a user group that has appropriate permission policies attached (recommended), or by directly attaching policies to the user.

Additional information:

An IAM role is similar to an IAM 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 (or any service, application, ...etc) who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session. IAM roles are meant to be assumed by authorized entities, such as IAM users, applications, or an AWS service such as Amazon EC2.

"AWS Organizations" is incorrect. AWS Organizations can be used to group AWS accounts, not IAM users (the employees). AWS Organization helps you to centrally manage billing; control access, compliance, and security; and share resources across multiple AWS accounts.

References:

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

Question 63:

Skipped

What does the AWS Health Dashboard provide? (Choose TWO)

- **Health checks for Auto Scaling instances**
- **Personalized view of AWS service health**

  (Correct)

- **A dashboard detailing vulnerabilities in your applications**
- **Detailed troubleshooting guidance to address AWS events impacting your resources**

  (Correct)

- **Recommendations for Cost Optimization**

Explanation

The AWS Health Dashboard (previously AWS Personal Health Dashboard) is the single place to learn about the availability and operations of AWS services. You can view the overall status of all AWS services, and you can sign in to access a personalized view of the health of the specific services that are powering your workloads and applications. AWS Health Dashboard proactively notifies you when AWS experiences any events that may affect you, helping provide quick visibility and guidance to minimize the impact of events in progress, and plan for any scheduled changes, such as AWS hardware maintenance.

The benefits of the AWS Health Dashboard include:

**A personalized View of Service Health: Personal Health Dashboard gives you a personalized view of the status of the AWS services that power your applications, enabling you to quickly see when AWS is experiencing issues that may impact you.

For example, in the event of a lost EBS volume associated with one of your EC2 instances, you would gain quick visibility into the status of the specific service you are using, helping save precious time troubleshooting to determine root cause.

**Proactive Notifications: The dashboard also provides forward looking notifications, and you can set up alerts across multiple channels, including email and mobile notifications, so you receive timely and relevant information to help plan for scheduled changes that may affect you. In the event of AWS hardware maintenance activities that may impact one of your EC2 instances, for example, you would receive an alert with information to help you plan for, and proactively address any issues associated with the upcoming change.

**Detailed Troubleshooting Guidance: When you get an alert, it includes remediation details and specific guidance to enable you to take immediate action to address AWS events impacting your resources. For example, in the event of an AWS hardware failure impacting one of your EBS volumes, your alert would include a list of your affected resources, a recommendation to restore your volume, and links to the steps to help you restore it from a snapshot. This targeted and actionable information reduces the time needed to resolve issues.

The other options are incorrect:

"A dashboard detailing vulnerabilities in your applications" is incorrect. You can check your applications for vulnerabilities using other services such as Amazon Inspector.

"Recommendations for Cost Optimization" is incorrect. You can get help about cost optimization using other services such as the AWS Trusted Advisor.

"Health checks for Auto Scaling instances" is incorrect. AWS Health Dashboard does not provide instance health checks. Amazon EC2 Auto Scaling can determine the health status of an instance by using one or more of the following health checks:

1- Amazon EC2 status checks and scheduled events: Checks that the instance is running; checks for underlying hardware or software issues that might impair the instance.

2- Elastic Load Balancing health checks: Checks whether the load balancer reports the instance as healthy, confirming whether the instance is available to handle requests.

3- Custom health checks: Checks for any other problems that might indicate instance health issues, according to your custom health checks.

The health status of an Auto Scaling instance indicates whether it is healthy or unhealthy. All instances in your Auto Scaling group start in the healthy state. Instances are assumed to be healthy unless Amazon EC2 Auto Scaling receives notification that they are unhealthy. This notification can come from sources such as Amazon EC2, Elastic Load Balancing, or custom health checks. When Amazon EC2 Auto Scaling detects an unhealthy instance, it terminates it and launches a new one.

References:

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

Question 64:

Skipped

How can you view the distribution of AWS spending in one of your AWS accounts?

- **By contacting the AWS Finance team**
- **By using AWS Cost Explorer**

  (Correct)

- **By contacting the AWS Support team**
- **By using Amazon VPC console**

Explanation

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 12 months, and get recommendations for what Reserved Instances to purchase. 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. You can also specify time ranges for the data, and view time data by day or by month.

The other options are incorrect:

"By contacting the AWS Finance team" is incorrect. The AWS Finance Team provides data driven analysis, strategic decision support, financial planning, and controllership to teams that plan and build data centers, design and source servers, and develop and sell cloud services at massive scale to developers and businesses all over the world.

"By contacting the AWS Support team" is incorrect. The AWS support team will direct you to use AWS Cost Explorer.

"By using Amazon VPC console" is incorrect. You can use the Amazon Virtual Private Cloud console to launch AWS resources, such as Amazon EC2 instances. You can use it to specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.

References:

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

Question 65:

Skipped

What is the AWS feature that provides an additional level of security above the default authentication mechanism of usernames and passwords?

- **AWS MFA**

  (Correct)

- **Email verification**
- **Encrypted keys**
- **AWS KMS**

Explanation

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.

The other options are incorrect:

"Encrypted keys" is incorrect. Logging into the AWS management console doesn’t require encrypted keys.

"Email verification" is incorrect. Email verification is the process of verifying your ownership of an account’s e-mail address.

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

References:

https://aws.amazon.com/iam/details/mfa/