

What does AWS Snowball provide? (Choose TWO)

- A hybrid cloud storage between on-premises environments and the AWS Cloud
- An Exabyte-scale data transfer service that allows you to move extremely large amounts of data to AWS

(Incorrect)

- A catalog of third-party software solutions that customers need to build solutions and run their businesses

(Incorrect)

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

(Correct)

- Built-in computing capabilities that allow customers to process data locally

(Correct)

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 2: **Correct**

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

-
-

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

-
-

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

(Correct)

-
-

The on-demand instances follow the AWS pay-as-you-go pricing model

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 3: **Incorrect**

What is the AWS service that enables AWS architects to manage infrastructure as code?

-

Amazon EMR

(Incorrect)

-

AWS CloudFormation

(Correct)

-

AWS Config

- ○

Amazon SES

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:

[#### Question 4: **Incorrect**](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide>Welcome.html</p></div><div data-bbox=)

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?



Elastic RI



Convertible RI

(Correct)



Premium RI



Standard RI

(Incorrect)

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 5: Correct

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)

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

(Correct)

- Availability Zones

(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 6: **Correct**

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

- Email verification
- AWS MFA
(Correct)
- AWS KMS
- Encrypted keys

Explanation

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of using just your user name and password to authenticate.

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/>

Question 7: Incorrect

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 CloudWatch
- AWS OpsWorks

(Incorrect)

- Amazon Aurora

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 8: **Correct**

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 roles
- IAM Groups
- IAM users

(Correct)

Explanation

An IAM group is a collection of IAM users that are managed as a unit. 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 group called Admins and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to

the group. If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to that 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 groups and add him or her to the appropriate new 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 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 9: **Incorrect**

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 Security team

(Incorrect)

-

Contact the AWS Abuse team

(Correct)

-

Contact the AWS Concierge team

-

Contact the AWS Customer Service team

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 10: **Incorrect**

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



Dedicated instances



Spot instances

(Incorrect)



Reserved instances



On-demand instances

(Correct)

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 11: Incorrect

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

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

- ○

Each AWS account gets volume discounts

(Correct)

- ○

The consolidated billing feature is just for organizational purposes

(Incorrect)

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 12: **Correct**

Which of the following is an example of horizontal scaling in the AWS Cloud?

-
-

Adding more RAM capacity to an EC2 instance

-
-

Adding more EC2 instances of the same size to handle an increase in traffic

(Correct)

-
-

Increasing the compute capacity of a single EC2 instance to address the growing demands of an application

-
-

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 13: **Correct**

Which service provides DNS in the AWS cloud?

- AWS Config
- Route 53
- Amazon EMR
-

(Correct)

Amazon CloudFront

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 14: **Correct**

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



Amazon DynamoDB

(Correct)

-

Amazon Aurora

-

Amazon Redshift

-

Amazon Elastic Block Store

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: **Incorrect**

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

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

(Correct)

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: Incorrect

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

-

Patching the Network infrastructure

-

Configuring network access rules

(Correct)

-

Controlling physical access to compute resources

(Incorrect)

-

Disk disposal

-

Setting password complexity rules

(Correct)

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 17: **Incorrect**

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

- Increasing speed and agility

(Correct)

- There is no need to worry about security

(Incorrect)

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

(Correct)

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 18: **Incorrect**

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 Budgets
- AWS Elastic Load Balancer
(Incorrect)
- AWS Cost Explorer
- 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 19: **Incorrect**

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

(Incorrect)

-
-

AWS Storage Gateway

-
-

Amazon ElastiCache

(Correct)

-
-

AWS OpsWorks

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 20: **Incorrect**

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 Config



AWS WAF

(Correct)

Amazon Cognito



AWS Shield

(Correct)

AWS KMS

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 21: **Correct**

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

-

Amazon VPC

(Correct)

-

AWS VPN

-

AWS Subnets

-

AWS Dedicated Hosts

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 22: **Correct**

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



AWS SDK



AWS Management Console

(Correct)



AWS CLI



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 23: **Correct**

Which service provides object-level storage in AWS?

- - Amazon EFS
 -
 - Amazon Instance Store
 -
 - Amazon S3
- (Correct)**
-

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 24: **Correct**

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



Amazon S3 Intelligent-Tiering

(Correct)



Amazon S3 Standard



Amazon S3 Standard-Infrequent Access



Amazon S3 Glacier

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" is incorrect. Amazon S3 Glacier is a low-cost storage class for data that is rarely accessed; such as archived data.

References:

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

Question 25: **Correct**

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

- Adopt monolithic architecture
 - Implement elasticity
- (Correct)**
- Parallelize tasks
 - 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 26: **Correct**

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



Use AWS reservations to reduce costs when testing your production environment



Automate wherever possible to make architectural experimentation easier

(Correct)

-
-

Provision a large compute capacity to handle any spikes in load

-
-

Invest heavily in architecting your environment, as it is not easy to change your design later

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 5

Question 27: **Correct**

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

- ○

Software as a Service (SaaS)

-
- Infrastructure as a Service (IaaS)
-
- Platform as a Service (PaaS)
-
- Networking as a Service (NaaS)

(Correct)

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 28: **Incorrect**

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

(Incorrect)

-
-

Deploy the application across multiple Regions and Availability Zones

(Correct)

-
-

Deploy the application across multiple VPC's and subnets

-
-

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 29: **Correct**

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

-

AWS Artifact

(Correct)

-

AWS Certificate Manager

- ○
AWS Organizations
- ○
AWS Systems Manager

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 30: **Correct**

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

-

All AWS services are considered Global Services, and this design helps customers serve their international users

-

Ability to recover quickly from failures

(Correct)

-

Applying the principle of least privilege to all AWS resources

-

Automatically provisioning new resources to meet demand

(Correct)

-

Providing compensation to customers if issues occur

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 31: **Correct**

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

- IAM users should not be granted any permissions; to keep your account safe
- All IAM users should have at least the necessary permissions to access the core AWS services
- All trusted IAM users should have access to any AWS service in the respective AWS account
- You should grant your users only the permissions they need when they need them and nothing more

(Correct)

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 32: **Incorrect**

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?

-
-

The purchased instances will have better performance than On-demand instances

-
-

All accounts can receive the hourly cost benefit of the Reserved Instances

(Correct)

-
-

The Reserved Instance discounts can only be shared with the master account

-
-

There are no cost benefits from using consolidated billing; It is for informational purposes only

(Incorrect)

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 33: **Incorrect**

Select TWO examples of the AWS shared controls.

-

IAM Management

(Incorrect)

-

Data Center operations

-

VPC Management

-

Patch Management

(Correct)

-

Configuration Management

(Correct)

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 34: **Correct**

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?

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

Amazon S3 Glacier Deep Archive

(Correct)

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 35:

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 Simple Email Service to send billing alerts to their email address on a daily basis
- Setup a CloudWatch billing alarm that triggers an SNS notification when the threshold is exceeded

(Correct)

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

(Correct)

- Configure AWS CloudTrail to automatically delete all AWS resources when the threshold is exceeded
- Configure the Amazon Connect Service to alert the company when the threshold is exceeded

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 36: **Correct**

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

-
-

By using AWS Cost Explorer

(Correct)

-
-

By contacting the AWS Finance team

-
-

By using Amazon VPC console

-
-

By contacting the AWS Support team

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 37:

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 CloudWatch
- Amazon RDS
- (Correct)**
 - Amazon Redshift
 - 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 38:

Skipped

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

-

Ensure that EBS data is encrypted at rest

(Correct)

-

Regularly update firmware on EBS devices

-

Store a backup daily in an external drive

-

Create EBS snapshots

(Correct)

-

Prevent any unauthorized access to AWS data centers

Explanation

Creating snapshots of EBS Volumes can help ensure that you have a backup of your EBS volumes just in case any issues arise.

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 39: **Correct**

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 SNS
- Amazon Kinesis Video Streams
- AWS CloudFormation
- Amazon CloudFront

(Correct)

Explanation

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, 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 40: **Correct**

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?



Reserved Instances



Spot Instances

(Correct)



On-demand Instances



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 that 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 41: **Correct**

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 CloudTrail

- -
 -
 -
 -
- AWS Lambda
- AWS Config
- 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 42: **Correct**

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 Config



IAM Groups



AWS Organizations

(Correct)



AWS Trusted Advisor

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 policies 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 Groups" is incorrect. IAM groups are not used to manage multiple AWS accounts. An IAM group is a collection of IAM users - within the same AWS account - that are managed as a unit. IAM 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 group called Admins and give that 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 43: **Incorrect**

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

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

(Correct)

-

AWS Budgets

(Incorrect)

-

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 44: **Incorrect**

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

-
-

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

(Incorrect)

-
-

Penetration testing can be performed by the customer on their own instances without prior authorization from AWS

(Correct)

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 WorkSpaces, 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 45: **Correct**

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

- AWS Availability Zones
- AWS Global Accelerator
- AWS Edge Locations

(Correct)

- AWS Regions

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 46: **Correct**

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?

-
-

AWS Support Concierge Service

-
-

AWS Knowledge Center

• Infrastructure Event Management

(Correct)

• AWS Personal 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 Personal Health Dashboard" is incorrect. AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

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 47: Correct

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

-

Access keys

(Correct)

-

Secret token

-

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 48: Incorrect

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

-

Amazon S3 provides unlimited storage for any type of data

-

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 provides 99.999999999% (11 9's) of data durability

-

Amazon S3 stores any number of objects, but with object size limits

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 99.99999999% 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 49: **Correct**

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 Shield
- AWS Secrets Manager
- AWS Management Console
- AWS Trusted Advisor

(Correct)

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 50: **Incorrect**

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?

- Registering a new US domain name to serve the users in the US
- Deploying new Amazon EC2 instances in a Region located in the US
(Correct)
- Building a new data center in the US and implementing a hybrid model
- Applying the Amazon Connect latency-based routing policy
(Incorrect)

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 51: **Incorrect**

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 scaling your AWS resources using an Elastic Load Balancer

(Incorrect)

-

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 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 52: **Incorrect**

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 MapReduce

(Correct)

-

Amazon VPC

-

Amazon DynamoDB

(Correct)

-

Amazon Elastic Compute Cloud

(Incorrect)

-

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, 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 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 53: **Incorrect**

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)

- Auto Scaling

(Correct)

- ECR

(Incorrect)

- Amazon Athena
-

ELB

(Correct)

-

Amazon EC2

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 (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 54: **Correct**

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 Inspector

(Correct)

-

Amazon SNS

-

Concierge Support Team

-

AWS Trusted Advisor

(Correct)

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 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 55: **Incorrect**

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

- Recommendations for Cost Optimization
- A dashboard detailing vulnerabilities in your applications
- Published information about the current status and availability of all AWS services

(Incorrect)

- Detailed troubleshooting guidance to address AWS events impacting your resources

(Correct)

- Personalized view of AWS service health

(Correct)

Explanation

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The benefits of the AWS personal 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.

"Published information about the current status and availability of all AWS services" is incorrect. You can get information about the current status and availability of the AWS services any time using the AWS Service Health Dashboard that is available at this link: <https://status.aws.amazon.com/>

References:

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

Question 56: **Correct**

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



Amazon SES



AWS Direct Connect



Amazon SQS

(Correct)



Amazon 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 57: **Incorrect**

Which statement is true regarding the AWS Shared Responsibility Model?

- Patching the guest OS is always the responsibility of AWS
- Security of the IaaS services is the responsibility of AWS
- (Incorrect) Security of the managed services is the responsibility of the customer
- Responsibilities vary depending on the services used

(Correct)

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, Amazon VPC, and Amazon S3—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, Amazon Elastic MapReduce, and Amazon WorkSpaces. 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 58: **Correct**

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

-
-

Amazon DynamoDB

(Correct)

-
-

Amazon Redshift

-
-

Amazon Aurora

-
-

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 59: **Correct**

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

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

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 60: **Incorrect**

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?

-
-

AWS Trusted Advisor

-
-

Amazon Inspector

(Incorrect)

-
-

AWS CloudTrail

(Correct)

• ○

EC2 Instance Usage Report

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 61: **Incorrect**

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

- ○
Allows updates of any monolithic application quickly and easily
- ○
Reduces inter-dependencies so that failures do not impact other components of the application

(Correct)

- ○
Allows tracking of any API call made to any AWS service

(Incorrect)

- ○
Allows treating an application as a single, cohesive unit

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 62: Incorrect

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

(Incorrect)

-
-

Amazon Neptune

-
-

A MySQL database installed on an EC2 instance

-
-

Amazon Aurora

(Correct)

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 63: **Incorrect**

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 Operations Support

-

AWS Support Concierge

(Correct)

-

AWS Personal Health Dashboard

-

AWS Customer Service

(Incorrect)

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 inquiries.

** 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 Personal Health Dashboard" is incorrect. AWS Personal Health Dashboard provides a personalized view of the health of the specific services that are powering your workloads and applications. AWS Personal 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 64: **Correct**

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 Database Migration Service

(Correct)

-

AWS Server Migration Service

-

AWS Application Discovery Service

-

AWS OpsWorks

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 65: **Correct**

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

-

Server-side encryption

-

Configuring infrastructure devices

(Correct)

-

Client-side encryption

-

Filtering traffic with Security Groups

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/>

Continue

Retake test

Question 1: **Incorrect**

Which of the following aspects of security are managed by AWS? (Choose TWO)

- Access permissions
- VPC security

(Incorrect)

- Hardware patching

(Correct)

- Encryption of EBS volumes
- Securing global physical infrastructure

(Correct)

Explanation

AWS is continuously innovating the design and systems of its data centers to protect them from man-made and natural risks. For example, at the first layer of security, AWS provides a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

According to the Shared Responsibility model, patching of the underlying hardware is the AWS' responsibility. AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

The other options are incorrect:

"VPC security" is incorrect. The configuration and security of the VPC are customer's responsibilities.

"Encryption of EBS volumes" is incorrect. The customer is responsible for encrypting their data on EBS either on the client side or on the server side.

"Access permissions" is incorrect. The customer is responsible for managing the IAM permissions.

Additional information:

IAM permissions let the customer specify access to AWS resources. Permissions are granted to IAM entities (users, groups, and roles) and by default these entities start with no permissions. In other words, IAM entities can do nothing in AWS until you grant them your desired permissions. To give entities permissions, you can attach a policy that specifies the type of access, the actions that can be performed, and the resources on which the actions can be performed.

References:

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

Question 2: **Incorrect**

A company has deployed a new web application on multiple Amazon EC2 instances. Which of the following should they use to ensure that the incoming HTTP traffic is distributed evenly across the instances?



AWS Auto Scaling



AWS Network Load Balancer

(Incorrect)



AWS EC2 Auto Recovery

-
- AWS Application Load Balancer
(Correct)

Explanation

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. Elastic Load Balancing offers four types of load balancers: 1- Application Load Balancer. 2- Network Load Balancer. 3- Gateway Load Balancer. 4- Classic Load Balancer. Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic. In our case, the application receives HTTP traffic. Hence, the Application Load Balancer is the correct answer here.

The other options are incorrect:

"AWS Network Load Balancer" is incorrect. The traffic comes to the instances through HTTP. Network Load Balancer is best suited for load balancing of TCP and TLS traffic.

"AWS Auto Scaling" is incorrect. AWS Auto Scaling is not for distributing traffic. AWS Auto Scaling monitors your applications and automatically adjusts capacity (up or down) to maintain steady, predictable performance at the lowest possible cost.

"AWS EC2 Auto Recovery" is incorrect. Auto Recovery is an Amazon EC2 feature that is designed to increase instance availability. Auto Recovery can be configured to automatically recover EC2 Instances when a system or hardware impairment is detected.

References:

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

Question 3: **Incorrect**

According to the AWS Shared responsibility model, which of the following are the responsibility of the customer? (Choose TWO)

- Managing environmental events of AWS data centers
 - Ensuring that the underlying EC2 host is configured properly
- (Incorrect)**
- Controlling physical access to AWS Regions
 - Protecting the confidentiality of data in transit in Amazon S3

(Correct)

- Patching applications installed on Amazon EC2

(Correct)

Explanation

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in AWS data centers). The AWS customer is responsible for protecting their data **either at rest or in transit** for all services (including S3).

Patch management is a shared control between AWS and the customer. AWS is responsible for patching the underlying hosts, updating the firmware, and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications.

The other options are incorrect:

"Ensuring that the underlying EC2 host is configured properly" is incorrect. Configuration management is a shared control between AWS and the customer. AWS maintains the configuration of the underlying hosts and its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

"Managing environmental events of AWS data centers" is incorrect. It is the sole responsibility of AWS to manage these environmental events.

"Controlling physical access to AWS regions" is incorrect. It is the sole responsibility of AWS to control physical access to its data centers.

References:

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

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

Question 4: **Incorrect**

Which of the following EC2 instance purchasing options supports the Bring Your Own License (BYOL) model for almost every BYOL scenario?

-
-

Dedicated Hosts

(Correct)

-
-

Dedicated Instances

-
-

Reserved Instances

(Incorrect)

On-demand Instances

Explanation

You have a variety of options for using new and existing Microsoft software licenses on the AWS Cloud. By purchasing Amazon Elastic Compute Cloud (Amazon EC2) or Amazon Relational Database Service (Amazon RDS) license-included instances, you get **new**, fully compliant Windows Server and SQL Server licenses from AWS. The BYOL model enables AWS customers to use their **existing** server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server.

Your **existing** licenses may be used on AWS with Amazon EC2 Dedicated Hosts, Amazon EC2 Dedicated Instances or EC2 instances with default tenancy using Microsoft License Mobility through Software Assurance.

Dedicated Hosts provide additional control over your instances and visibility into Host level resources and tooling that allows you to manage software that consumes licenses on a per-core or per-socket basis, such as Windows Server and SQL Server. This is why most BYOL scenarios are supported through the use of Dedicated Hosts, while only certain scenarios are supported by Dedicated Instances.

The other options are incorrect:

"Dedicated Instances" is incorrect. Dedicated Hosts is recommended for most BYOL scenarios for the reasons we mentioned above.

"On-demand Instances" and "Reserved Instances" are incorrect. On-demand instance and Reserved instances don't support the Bring Your Own License (BYOL) model.

References:

<https://aws.amazon.com/ec2/dedicated-hosts/>

Question 5: **Correct**

Which of the below is a best-practice when building applications on AWS?

- Ensure that the application runs on hardware from trusted vendors
 - Use IAM policies to maintain performance
 -
- Decouple the components of the application so that they run independently

(Correct)

-
- Strengthen physical security by applying the principle of least privilege

Explanation

An application should be designed in a way that reduces interdependencies between its components. A change or a failure in one component should not cascade to other components. If the components of an application are tightly-coupled (interconnected) and one component fails, the entire application will also fail. **Amazon SQS** and **Amazon SNS** are powerful tools that help you build loosely-coupled applications. SQS and SNS can be integrated together to decouple application components so that they run independently, increasing the overall fault tolerance of the application.

Understanding how SQS and SNS services work is not required for the Cloud Practitioner level, but let's just take a simple example, let say you have two components in your application, Component A & Component B. Component A sends messages (jobs) to component B to process. Now, what happens if component A sends a large number of messages at the same time? Component B will fail, and the entire application will fail. SQS act as a middleman, receives and stores messages from component A, and component B pull and process messages at its own pace. This way, both components run independently from each other.

The other options are incorrect:

"Ensure that the application runs on hardware from trusted vendors" is incorrect. Choosing a specific hardware vendor is not available in AWS.

"Use IAM policies to maintain performance" is incorrect. There is no relation between IAM policies and performance. IAM policies are used to grant users permission to perform specific actions on AWS.

"Strengthen physical security by applying the principle of least privilege" is incorrect. Physical security is the sole responsibility of AWS.

Additional information:

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires.

The principle of least privilege does not only apply to control physical access. AWS customers should also apply this principle when granting permissions to IAM users. In other words, AWS customers should grant IAM users only the permissions they need to perform a task and nothing more.

References:

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

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

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

Question 6: **Incorrect**

Which of the following activities may help reduce your AWS monthly costs? (Choose TWO)

-
-

Enabling Amazon EC2 Auto Scaling for all of your workloads

(Correct)

-

Removing all of your Cost Allocation Tags

-

Creating a lifecycle policy to move infrequently accessed data to less expensive storage tiers

(Correct)

-

Using the AWS Network Load Balancer (NLB) to load balance the incoming HTTP requests

-

Deploying your AWS resources across multiple Availability Zones

(Incorrect)

Explanation

Amazon EC2 Auto Scaling monitors your applications and automatically adjusts capacity (up or down) to maintain steady, predictable performance at the lowest possible cost. When demand drops, Amazon EC2 Auto Scaling will automatically remove any excess capacity so you avoid overspending. When demand increases, Amazon EC2 Auto Scaling will automatically add capacity to maintain performance.

For Amazon S3 and Amazon EFS, you can create a lifecycle policy to automatically move infrequently accessed data to less expensive storage tiers. In order to reduce your Amazon S3 costs, you should create a lifecycle policy to automatically move old (or infrequently accessed) files to less expensive storage tiers such as Amazon Glacier, or to automatically delete them after a specified duration. Similarly, you can create an Amazon EFS lifecycle policy to automatically move less frequently accessed data to less expensive storage tiers such as Amazon EFS Standard-Infrequent Access (EFS Standard-IA) and Amazon EFS One Zone-Infrequent Access (EFS One Zone-IA). Amazon EFS Infrequent Access storage classes provide price/performance that is cost-optimized for files not accessed every day, with storage prices **up to 92% lower** compared to Amazon EFS Standard (EFS Standard) and Amazon EFS One Zone (EFS One Zone) storage classes respectively.

The other options are incorrect:

"Removing all of your Cost Allocation Tags" is incorrect. A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a *key* and a *value*. For each resource, each tag key must be unique, and each tag key can have only one value. You can use tags to organize your resources (by project, team, ...etc.), and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs. Removing all of your Cost Allocation Tags will not help reduce your AWS monthly costs.

"Deploying your AWS resources across multiple Availability Zones" is incorrect. Deploying your AWS resources across multiple Availability Zones can help increase your application's availability and fault-tolerance.

"Using the AWS Network Load Balancer (NLB) to load balance the incoming HTTP requests" is incorrect. This option is incorrect for two reasons:

1st: Load Balancing does not reduce costs, Elastic Load Balancing automatically distributes incoming application traffic evenly across multiple targets, such as Amazon EC2 instances, containers, and Lambda functions, and helps you gain more consistent application performance.

2nd: The recommended Load Balancer for HTTP traffic is the AWS Application Load Balancer, NOT the AWS Network Load Balancer.

Additional information:

Elastic Load Balancing supports four types of load balancers (Application Load Balancer, Network Load Balancer, Gateway Load Balancer, and Classic Load Balancer). You can select the appropriate load balancer based on your application needs.

1- If you need to load balance HTTP\HTTPS requests, AWS recommends using the Application Load Balancer.

2- For network/transport protocols (layer4 – TCP, UDP) load balancing, and for extreme performance/low latency applications, AWS recommends using Network Load Balancer.

3- To manage and distribute traffic across multiple third-party virtual appliances, AWS recommends using the Gateway Load Balancer.

4- If you have an existing application built within the EC2-Classic network, you should use a Classic Load Balancer.

References:

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

<https://aws.amazon.com/efs/features/infrequent-access/>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html>

Question 7: **Incorrect**

Which of the following services will help businesses ensure compliance in AWS?

-

CloudFront

(Incorrect)

-

CloudTrail

(Correct)

-

CloudEndure Migration

-

CloudWatch

Explanation

AWS CloudTrail is designed to log all actions taken in your AWS account. This provides a great resource for governance, compliance, and risk auditing.

The other options are incorrect:

"CloudFront" is incorrect. Amazon CloudFront is a content delivery network (CDN) service.

"CloudEndure Migration" is incorrect. CloudEndure Migration simplifies the process of migrating applications from physical, virtual, and cloud-based infrastructure, ensuring that they are fully operational in any AWS Region without compatibility issues.

"CloudWatch" is incorrect. Amazon CloudWatch is used to monitor the utilization of AWS resources. CloudWatch provides you with data and actionable insights to monitor your applications, understand and respond to system-wide performance changes, and get a unified view of operational health.

References:

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

Question 8: **Correct**

A company needs to host a database in Amazon RDS for at least three years. Which of the following options would be the most cost-effective solution?

-
-

Reserved instances - Partial Upfront

(Correct)

-
-

Reserved instances - No Upfront

-
-

On-Demand instances

• ○

Spot Instances

Explanation

Since the database server will be hosted for a period of at least three years, then it is better to use the RDS Reserved Instances as it provides you with a significant discount compared to the On-Demand Instance pricing for the DB instance.

With the Partial Upfront option, you make a low upfront payment and are then charged a discounted hourly rate for the instance for the duration of the Reserved Instance term. The Partial Upfront option is more cost-effective than the No upfront option (The more you spend upfront the more you save).

The other options are incorrect:

"Spot Instances" is incorrect. Spot Instances is an option for EC2; there is no Spot option for RDS.

"Reserved instances - No Upfront" is incorrect. The No Upfront option does not require any upfront payment and provides a discounted hourly rate for the duration of the term. The Partial Upfront option provides more discounts than the No Upfront option because you spend more upfront.

"On-Demand instances" is incorrect. On-Demand is not a cost-effective solution.

References:

<https://aws.amazon.com/rds/reserved-instances/>

Question 9: **Correct**

Which AWS service can be used to store and reliably deliver messages across distributed systems?



Amazon Simple Email Service

-

Amazon Simple Storage Service

-

Amazon Simple Queue Service

(Correct)

-

AWS Storage Gateway

Explanation

Amazon SQS is a highly reliable, scalable message queuing service that enables asynchronous message-based communication between distributed components of an application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

The other options are incorrect:

"Amazon Simple Storage Service" is incorrect. Amazon Simple Storage Service (Amazon S3) is an object storage service.

"Amazon Simple Email Service" 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.

"AWS Storage Gateway" is incorrect. AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. The gateway connects to AWS storage services - such as Amazon S3 and Amazon EBS - and provides storage for files, volumes, snapshots, and virtual tapes in AWS.

References:

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

Question 10: **Correct**

Which of the following can help protect your EC2 instances from DDoS attacks?
(Choose TWO)

-

AWS CloudHSM

-

Network Access Control Lists (Network ACLs)

(Correct)

-

Security Groups

(Correct)

-

AWS Batch

-

AWS IAM

Explanation

Malicious actors sometimes use distributed denial of service (DDoS) attacks to flood a network, system, or application with more traffic, connections, or requests than it can handle.

When dealing with DDoS attacks, it is important to minimize the opportunities an attacker has to target your applications. This means restricting the type of traffic that can reach your applications. Configuring security groups and network ACLs in Amazon VPC is an effective tool to help filter traffic, and reduce the attack surface of your applications.

Security groups allow you to control inbound and outbound traffic to your Amazon EC2 instances by specifically allowing communication only on the ports and

protocols required for your applications. Access to any other port or protocol is automatically denied.

Network ACLs provide an additional layer of defense for your VPC by allowing you to create allow and deny rules that are processed in numeric order, much like a traditional firewall. This is useful for allowing or denying traffic at a subnet level, as opposed to security groups that filter traffic at an EC2 instance level. For example, if you have identified Internet IP addresses or ranges that are unwanted or potentially abusive, you can block them from reaching your application with a Network ACL deny rule.

Additional information:

AWS does not configure security groups or Network ACLs to protect you from DDoS attacks. It is the responsibility of the customer to set the appropriate Network ACL and security group rules to protect from these attacks and secure their network.

In addition to Security Groups and Network ACLs, 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:

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

"AWS IAM" is incorrect. AWS IAM enables you to manage access to AWS services and resources securely.

"AWS Batch" is incorrect. AWS Batch is a compute service that allows you to run hundreds of thousands of batch computing jobs on AWS.

References:

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

Question 11: **Incorrect**

Which statement is correct with regards to AWS service limits? (Choose TWO)

- There are no service limits on AWS
- The Amazon Simple Email Service is responsible for sending email notifications when usage approaches a service limit

(Incorrect)

- Each IAM user has the same service limits
- You can contact AWS support to increase the service limits

(Correct)

- You can use the AWS Trusted Advisor to monitor your service limits

(Correct)

Explanation

Service limits, also referred to as **Service quotas**, are the maximum number of service resources or operations that apply to an AWS account. Understanding your service limits (and how close you are to them) is an important part of managing your AWS deployments – continuous monitoring allows you to request limit increases or shut down resources before the limit is reached. One of the easiest ways to do this is via **AWS Trusted Advisor's Service Limit Dashboard**.

AWS maintains service limits for each account to help guarantee the availability of AWS resources, as well as to minimize billing risks for new customers. Some service limits are raised automatically over time as you use AWS, though most AWS services require that you request limit increases manually. Most service limit increases can be requested through the AWS Support Center by choosing Create Case and then choosing Service Limit Increase.

The other options are incorrect:

"There are no service limits on AWS" is incorrect. Each AWS account has default limits, for each AWS service.

"The Amazon Simple Email Service is responsible for sending email notifications when usage approaches a service limit" 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.

Additional information:

You can configure the AWS Limit Monitor to send email notification when usage approaches a service limit.

"Each IAM user has the same service limits" is incorrect. Service limits are applied at the AWS account level by aggregating usage from all users in the account.

Note: "service limits" and "service quotas" are the exact same thing. Please note that you may encounter both terms being used interchangeably.

References:

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

<https://aws.amazon.com/answers/account-management/limit-monitor/>

<https://docs.aws.amazon.com/servicequotas/latest/userguide/intro.html>

Question 12: **Incorrect**

A company is migrating its on-premises database to Amazon RDS. What should the company do to ensure Amazon RDS costs are kept to a minimum?



Use a Multi-Region Active-Passive architecture



Combine On-demand Capacity Reservations with Saving Plans

(Incorrect)



Use a Multi-Region Active-Active architecture



Right-size before and after migration

(Correct)

Explanation

Right-sizing is the process of matching instance types and sizes to your workload performance and capacity requirements at the lowest possible cost. By right-sizing before migration, you can significantly reduce your infrastructure costs. If you skip right-sizing to save time, your migration speed might be faster, but you will end up with higher cloud infrastructure spend for a potentially long time.

Because your resource needs are always changing, right-sizing must become an ongoing process to continually achieve cost optimization. It's important to right-size when you first consider moving to the cloud and calculate the total cost of ownership. However, it's equally important to right-size periodically once you're in the cloud to ensure ongoing cost-performance optimization.

Picking an Amazon RDS instance for a given workload means finding the instance family that most closely matches the CPU, disk I/O, and memory needs of your

workload. Amazon RDS provides a wide selection of instances, which gives you lots of flexibility to right-size your resources to match capacity needs at the lowest cost.

The other options are incorrect:

"Use a Multi-Region Active-Active architecture" is incorrect. With the Multi-Region Active-Active solution, your workload is deployed to, and actively serving traffic from, multiple AWS Regions. AWS Customers use this approach to reduce latency for global users and achieve the highest level of availability. Using a Multi-Region Active-Active architecture will increase infrastructure costs, including Amazon RDS costs.

"Use a Multi-Region Active-Passive architecture" is incorrect. With Multi-Region Active-Passive architecture, your workload is deployed to two AWS Regions (a primary Region and a standby Region). In this architecture, user requests are served from the primary Region only. If the primary Region goes down because of a natural disaster or any other reason, the other Region will still be available and serve user requests. AWS customers use this approach for disaster recovery purposes. Using a Multi-Region Active-Passive architecture will increase infrastructure costs, including Amazon RDS costs.

"Combine On-demand Capacity Reservations with Saving Plans" is incorrect. When you combine On-demand Capacity Reservations with Saving Plans, you will be able to reduce costs significantly. But, On-demand Capacity Reservations is available only for Amazon EC2. For more information about On-demand Capacity Reservations, check this link: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html>

References:

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-right-sizing/right-size-before-migrating.html>

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-right-sizing/conclusion.html>

Question 13: **Incorrect**

An organization needs to analyze and process a large number of data sets. Which AWS service should they use?

-

Amazon MQ

(Incorrect)

-

Amazon SNS

-

Amazon EMR

(Correct)

-

Amazon SQS

Explanation

Amazon EMR helps you analyze and process vast amounts of data by distributing the computational work across a cluster of virtual servers running in the AWS Cloud. The cluster is managed using an open-source framework called Hadoop. Amazon EMR lets you focus on crunching or analyzing your data without having to worry about time-consuming setup, management, and tuning of Hadoop clusters or the compute capacity they rely on.

All other options are AWS messaging services.

References:

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

Question 14: **Correct**

What is the AWS tool that enables you to use scripts to manage all AWS services and resources?



AWS OpsWorks



AWS Console



AWS Service Catalog



AWS CLI

(Correct)

Explanation

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.

The other options are incorrect:

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

"AWS OpsWorks" is incorrect. AWS OpsWorks can be used to automate one service which is EC2. 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.

"AWS Console" is incorrect. AWS Console lets you access and manage Amazon Web Services through a web-based user interface.

References:

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

Question 15: **Incorrect**

In your on-premises environment, you can create as many virtual servers as you need from a single template. What can you use to perform the same in AWS?

-

An internet gateway

(Incorrect)

-

EBS Snapshot

-

IAM

-

AMI

(Correct)

Explanation

An Amazon Machine Image (AMI) is a template that contains a software configuration (for example, an operating system, an application server, and applications). This pre-configured template save time and avoid errors when configuring settings to create new instances. You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need. You can also launch instances from as many different AMIs as you need.

The other options are incorrect:

"IAM" is incorrect. IAM refers to the AWS Identity and Access Management.

"EBS Snapshot" is incorrect. An EBS snapshot is a point-in-time copy of your Amazon EBS volume.

"An internet gateway" is incorrect. An internet gateway is a VPC component that allows communication between instances in your VPC and the internet.

References:

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

Question 16: **Correct**

An organization runs many systems and uses many AWS products. Which of the following services enables them to control how each developer interacts with these products?

-
-

Amazon EMR

-
-

AWS Identity and Access Management

(Correct)

-
-

Network Access Control Lists

-
-

Amazon RDS

Explanation

AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.

The other options are incorrect:

"Amazon RDS" is incorrect. Amazon RDS is relational database service.

"Network Access Control Lists" is incorrect. Network Access Control Lists is a VPC feature that allows you to control traffic at the subnet level.

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

References:

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

Question 17: **Incorrect**

Which statement best describes the operational excellence pillar of the AWS Well-Architected Framework?

- The efficient use of computing resources to meet requirements
- The ability of a system to recover gracefully from failure

(Incorrect)

- The ability to manage datacenter operations more efficiently
- The ability to monitor systems and improve supporting processes and procedures

(Correct)

Explanation

The 5 Pillars of the AWS Well-Architected Framework:

1- Operational Excellence: The operational excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

2- Security: The security pillar includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

3- Reliability: The reliability pillar includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

4- Performance Efficiency: The performance efficiency pillar includes the ability to use computing resources efficiently to meet system requirements. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

5- Cost Optimization: The cost optimization pillar includes the ability to avoid or eliminate unneeded cost or sub-optimal resources.

Additional information:

Creating a software system is a lot like constructing a building. If the foundation is not solid, structural problems can undermine the integrity and function of the building. When architecting technology solutions on Amazon Web Services (AWS), if you neglect the five pillars of operational excellence, security, reliability, performance efficiency, and cost optimization, it can become challenging to build a system that delivers on your expectations and requirements. Incorporating these pillars into your architecture helps produce stable and efficient systems. This allows you to focus on the other aspects of design, such as functional requirements. The AWS Well-Architected Framework helps cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications.

The other options are incorrect:

"The ability of a system to recover gracefully from failure" is incorrect. This statement is much more related to the Reliability pillar.

"The efficient use of computing resources to meet requirements" is incorrect. This statement is much more related to the Performance Efficiency pillar.

"The ability to manage datacenter operations more efficiently" is incorrect. Managing datacenter operations is not related to any pillar. It is something that AWS is responsible for NOT the customer.

References:

<https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/>

Question 18: **Correct**

Which of the following AWS services can be used as a compute resource? (Choose TWO)

-

AWS Lambda

(Correct)

-

Amazon S3

-

Amazon EC2

(Correct)

-

Amazon VPC

-

Amazon CloudWatch

Explanation

AWS Lambda is a Serverless computing service. Serverless computing allows you to build and run applications and services without thinking about servers. With serverless computing, your application still runs on servers, but all the server management is done by AWS.

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, and resizable compute capacity in the cloud. Unlike AWS Lambda, Amazon EC2 is a server-based computing service, the Customer is responsible for performing all server configurations and management tasks.

The other options are incorrect:

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

Amazon VPC is incorrect. Amazon VPC is a networking service.

Amazon CloudWatch is incorrect. Amazon CloudWatch is a monitoring service.

References:

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

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

Question 19: **Correct**

Which AWS Service can be used to establish a dedicated, private network connection between AWS and your datacenter?

-

Amazon CloudFront

-

AWS Direct Connect

(Correct)

-

AWS Snowball

-

Amazon Route 53

Explanation

AWS Direct Connect is used to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or co-location environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

The other options are incorrect:

"AWS Snowball" is incorrect. AWS Snowball is used to physically migrate petabyte-scale data sets into and out of AWS.

"Amazon CloudFront" is incorrect. Amazon CloudFront is a content delivery network that provides faster response times for your global users.

"Amazon Route 53" is incorrect. Amazon Route 53 is a global service that provides a highly available and scalable Domain Name System (DNS) in the Cloud.

References:

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

Question 20: **Correct**

What are the default security credentials that are required to access the AWS management console for an IAM user account?



Security tokens



Access keys



MFA



A user name and password

(Correct)

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 only access the AWS management console if you have a valid user name and password.

The other options are incorrect:

"MFA" is incorrect. MFA is an additional layer of security (i.e. not required).

Although MFA is not required to access IAM user accounts, it is recommended to set it up for all of your IAM users. With MFA enabled, when a user signs in to an AWS Management Console, 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.

It is also recommended that you set an **IAM Account Password Policy** on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords.

You can configure an IAM Account Password Policy to do these things:

- 1- Set a minimum password length.
- 2- Require specific character types, including uppercase letters, lowercase letters, numbers, and non-alphanumeric characters. Be sure to remind your users that passwords are case sensitive.
- 3- Allow all IAM users to change their own passwords.
- 4- Require IAM users to change their password after a specified period of time (enable password expiration).
- 5- Prevent IAM users from reusing previous passwords.
- 6- Force IAM users to contact an account administrator when the user has allowed his or her password to expire.

Important Note: The IAM Account Password Policy is an account-level setting that applies to all IAM users, excluding the root user. You can not apply a password policy to a single IAM user.

"Access keys" is incorrect. Access keys are long-term credentials that can be used to sign programmatic requests to AWS.

"Security tokens" is incorrect. Security tokens are temporary credentials that can also be used to interact with AWS resources programmatically.

References:

<https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

Question 21: **Incorrect**

AWS has created a large number of Edge Locations as part of its Global Infrastructure. Which of the following is **NOT** a benefit of using Edge Locations?

- Edge locations are used by CloudFront to cache the most recent responses
- Edge locations are used by CloudFront to improve your end users' experience when uploading files

(Incorrect)

- Edge locations are used by CloudFront to distribute content to global users with low latency
- Edge locations are used by CloudFront to distribute traffic across multiple instances to reduce latency

(Correct)

Explanation

AWS Edge Locations are not used to distribute traffic. Edge Locations are used in conjunction with the CloudFront service to cache common responses and deliver content to end-users with low latency.

With Amazon CloudFront, your users can also benefit from accelerated content uploads. As the data arrives at an edge location, data is routed to AWS storage services over an optimized network path.

The AWS service that is used to distribute load is the AWS Elastic Load Balancing (ELB) service.

References:

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

Question 22: **Incorrect**

What does Amazon ElastiCache provide?

• An Ehcache compatible in-memory data store

(Incorrect)

• A domain name system in the cloud

• An online software store that allows Customers to launch pre-configured software with just few clicks

• In-memory caching for read-heavy applications

(Correct)

Explanation

ElastiCache is a web service that makes it easy to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. It provides a high-performance, scalable, and cost-effective caching solution, while removing the complexity associated with deploying and managing a distributed cache environment. The in-memory caching provided by Amazon ElastiCache can be used to significantly improve latency and throughput for many read-heavy applications (such as social networking, gaming, media sharing and Q&A portals) or compute-intensive workloads (such as a recommendation engine).

In-memory caching improves application performance by storing critical pieces of data in memory for low-latency access. Cached information may include the results of common database queries or the results of computationally-intensive calculations.

Additional information:

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:

"An online software store that allows Customers to launch pre-configured software with just few clicks" is **incorrect**. AWS Marketplace is the service that provides an online software store that helps customers find, buy, and immediately start using the software and services that run on AWS.

"A domain name system in the cloud" is **incorrect**. Route53 is the service that provides DNS in the cloud.

"An Ehcache compatible in-memory data store" is **incorrect**. ElastiCache supports only two cache engines: Redis and Memcached.

References:

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

Question 23: **Correct**

Which of the following is one of the benefits of moving infrastructure from an on-premises data center to AWS?

- AWS holds responsibility for managing customer applications
- Free support for all enterprise customers
- Automatic data protection

•

Reduced Capital Expenditure (CapEx)

(Correct)

Explanation

Capital expenditures (CapEx) are a company's major, long-term expenses, while operating expenses (OpEx) are a company's day-to-day expenses. Examples of CapEx include physical assets such as buildings, equipment, and machinery. Examples of OpEx include employee salaries, rent, utilities, and property taxes.

AWS enables businesses to leverage high-end technologies and infrastructure needs with **low CapEx and low OpEx**. The AWS pay-as-you-go model reduces investments in large capital expenditures. In addition, you can reduce the operating expense (OpEx) costs involved with the management and maintenance of data. This frees up budget, allowing you to quickly act on innovative initiatives that can't be easily pursued when managing physical data centers.

The other options are incorrect:

"Free support for all enterprise customers" is incorrect. Enterprise customers require access to technical support and other AWS support features. These support features are available only for paid support plans.

"Automatic data protection" is incorrect. Data protection is a customer responsibility. AWS customers have to decide which data should be public or private, set up how their data will be accessed, and decide whether this data will be encrypted or not and so on.

"AWS holds responsibility for managing customer applications" is incorrect. AWS customers are responsible for building, deploying, and managing their applications.

References:

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

Question 24: **Incorrect**

Which of the following are important design principles you should adopt when designing systems on AWS? (Choose TWO)

-

Always choose to pay as you go

(Incorrect)

-

Automate wherever possible

(Correct)

-

Treat servers as fixed resources

-

Always use Global Services in your architecture rather than Regional Services

-

Remove single points of failure

(Correct)

Explanation

A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. You can remove single points of failure by assuming everything will fail and designing your architecture to automatically detect and react to failures. For example, configuring and deploying an auto-scaling group of EC2 instances will ensure that if one or more of the instances crashes, Auto-scaling will automatically replace them with new instances. You should also introduce redundancy to remove single points of failure, by deploying your application across multiple Availability Zones. If one Availability Zone goes down for any reason, the other Availability Zones can serve requests.

AWS helps you use automation so you can build faster and more efficiently. Using AWS services, you can automate manual tasks or processes such as

deployments, development & test workflows, container management, and configuration management.

The other options are incorrect:

"Always choose to pay as you go" is incorrect. AWS has other payment models that can save you more costs depending on your use case. For example, If your application if your application has a steady state usage, you can use reservations for the Amazon RDS and Amazon EC2 instances to reduce your overall costs significantly.

"Treat servers as fixed resources" is incorrect. AWS enables you to treat your servers as disposable resources not fixed resources. This means that if any issue occurred with a server, you can simply replace it with a new one (rather trying to fix it).

"Always use Global services in your architecture rather than Regional services" is incorrect. AWS services\resources are either Global, Regional or specific to an Availability Zone. Among all the services\resources that AWS offers, only a few of them are considered global services. Examples of AWS global services include Amazon CloudFront, AWS Identity and Access Management, Amazon Route 53 and AWS WAF. There is no way you can build your AWS environment without using Regional services such as Amazon VPC, Amazon RDS, AWS Lambda and Amazon EFS OR Zonal resources (specific to an Availability Zone) such as Amazon EC2 instances or Amazon EBS volumes.

References:

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

Question 25: **Correct**

What is the AWS service\feature that takes advantage of Amazon CloudFront's globally distributed edge locations to transfer files to S3 with higher upload speeds?

- S3 Transfer Acceleration

(Correct)

- AWS WAF
- AWS Snowmobile
- AWS Snowball

Explanation

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

The other options are incorrect:

"AWS Snowball" is incorrect. AWS Snowball is a petabyte-scale data transport solution that uses devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud.

"AWS WAF" is incorrect. AWS WAF refers to the AWS Web Application Firewall service.

"AWS Snowmobile" is incorrect. AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>

Question 26: **Correct**

Based on the AWS Shared Responsibility Model, which of the following are the sole responsibility of AWS? (Choose TWO)

-

Creating hypervisors

(Correct)

-

Hardware maintenance

(Correct)

-

Configuring Access Control Lists (ACLs)

-

Installing software on EC2 instances

-

Monitoring network performance

Explanation

AWS is responsible for items such as the physical security of its data centers, creating hypervisors, replacement of old disk drives, and patch management of the infrastructure.

The customers are responsible for items such as building application schema, analyzing network performance, configuring security groups and network ACLs and encrypting their data.

References:

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

Question 27: **Correct**

Savings Plans are available for which of the following AWS compute services?
(Choose TWO)

- AWS Outposts
- Amazon Lightsail
- Amazon EC2
- AWS Batch
- AWS Lambda

(Correct)

Explanation

Savings Plans are a flexible pricing model that offers low prices on EC2, Lambda, and Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in \$/hour) for a 1 or 3 year term. When you sign up for Savings Plans, you will be charged the discounted Savings Plans price for your usage up to your commitment. For example, if you commit to \$10 of compute usage an hour, you will get the Savings Plans prices on that usage up to \$10 and any usage beyond the commitment will be charged On Demand rates.

Additional information:

What is the difference between Amazon EC2 Savings Plans and Amazon EC2 Reserved instances?

Reserved Instances are a billing discount applied to the use of On-Demand Compute Instances in your account. These On-Demand Instances must match certain attributes, such as instance type and Region to benefit from the billing discount.

For example, let say you have a t2.medium instance running as an On-Demand Instance and you purchase a Reserved Instance that matches the configuration of this particular t2.medium instance. At the time of purchase, the billing mode for the existing instance changes to the Reserved Instance discounted rate. The existing t2.medium instance doesn't need replacing or migrating to get the discount.

After the reservation expires, the instance is charged as an On-Demand Instance. You can repurchase the Reserved Instance to continue the discounted rate on your instance. Reserved Instances act as an automatic discount on new or existing On-Demand Instances in your account.

Savings Plans also offer significant savings on your Amazon EC2 costs compared to On-Demand Instance pricing. With Savings Plans, you make a commitment to a consistent usage amount, measured in USD per hour. This provides you with the flexibility to use the instance configurations that best meet your needs, instead of making a commitment to a specific instance configuration (as is the case with reserved instances). For example, with Compute Savings Plans, if you commit to \$10 of compute usage an hour, you can use as many instances as you need (of any type) and you will get the Savings Plans prices on that usage up to \$10 and any usage beyond the commitment will be charged On Demand rates.

The other options are incorrect:

"AWS Batch" is incorrect. Savings Plans are not available for AWS Batch.

AWS Batch is a compute service that allows you to run hundreds of thousands of batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted.

"AWS Outposts" is incorrect. Savings Plans are not available for AWS Outposts.

AWS Outposts is an AWS service that delivers the same AWS infrastructure, native AWS services, APIs, and tools to virtually any customer on-premises facility. With AWS Outposts, customers can run AWS services locally on their Outpost, including EC2, EBS, ECS, EKS, and RDS, and also have full access to services available in the Region.

Customers can use AWS Outposts to securely store and process data that needs to remain on-premises or in countries where there is no AWS region. AWS Outposts is ideal for applications that have low latency or local data processing requirements, such as financial services, healthcare, etc.

"Amazon Lightsail" is incorrect. Savings Plans are not available for Amazon Lightsail.

Amazon Lightsail provides a low-cost Virtual Private Server (VPS) in the cloud.

References:

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

Question 28: **Correct**

Which of the following services allows you to run containerized applications on a cluster of EC2 instances?

-
-

AWS Cloud9

-
-

Amazon ECS

(Correct)

-
-

AWS Personal Health Dashboard

-
-

AWS Data Pipeline

Explanation

Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers and allows you to easily run and scale containerized applications on AWS. Amazon ECS eliminates the need for you to install and operate your own container orchestration software, manage and scale a cluster of virtual machines, or schedule containers on those virtual machines.

The other options are incorrect.

"AWS Data Pipeline" is incorrect. AWS Data Pipeline is a web service that makes it easy to schedule regular data movement and data processing activities in the AWS cloud.

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

"AWS Personal Health Dashboard" is incorrect. AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.

References:

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

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

Question 29: **Correct**

What is the AWS serverless service that allows you to run your applications without any administrative burden?

- ○
Amazon RDS instances
- ●
AWS Lambda

(Correct)

- ○
Amazon LightSail
- ○
Amazon EC2 instances

Explanation

AWS Lambda is an AWS-managed compute service. It lets you run code without provisioning or managing servers. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code, and Lambda takes care of everything required to run and scale your code with high availability. You pay only for the compute time you consume - there is no charge when your code is not running.

The other options are incorrect:

"Amazon EC2 instances" is incorrect. Amazon Elastic Compute Cloud (Amazon EC2) is a server-based compute service. Amazon EC2 is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary configurations and management tasks.

"Amazon Lightsail" is incorrect. Amazon Lightsail provides a low-cost Virtual Private Server (VPS) in the cloud. Lightsail plans include everything you need to jumpstart your project – virtual machines, containers, databases, CDN, load balancers, SSD-based storage, DNS management, etc. – for a low, predictable monthly price.

"Amazon RDS instances" is incorrect. Amazon RDS is a server-based database service that makes it easy to run a relational database in the cloud.

References:

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

Question 30: **Correct**

You are working on two projects that require completely different network configurations. Which AWS service or feature will allow you to isolate resources and network configurations?

- Internet gateways
- Amazon CloudFront
- Security Groups
- Virtual Private Cloud

(Correct)

Explanation

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, including selection of the IP address range, creation of subnets, and configuration of route tables and network gateways.

"Security Groups" is incorrect. Security Groups are used to control traffic.

"Internet gateways" is incorrect. An internet gateway is a VPC component that allows communication between your VPC and the internet.

"Amazon CloudFront" is incorrect. Amazon CloudFront is a Content Delivery Network.

References:

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

Question 31: **Incorrect**

What is the primary storage service used by Amazon RDS database instances?



Amazon EFS



Amazon Glacier



Amazon S3

(Incorrect)



Amazon EBS

(Correct)

Explanation

DB instances for Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server use Amazon Elastic Block Store (Amazon EBS) volumes for database and log storage.

Additional information:

EBS volumes are performant for your most demanding workloads, including mission-critical applications such as SAP, Oracle, and Microsoft products. Amazon EBS scales with your performance needs, whether you are supporting millions of gaming customers or billions of e-commerce transactions. A broad range of workloads, such as relational databases (including Amazon RDS databases) and non-relational databases (including Cassandra and MongoDB), enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.

The other options are incorrect:

"Amazon S3" is incorrect. Amazon S3 refers to the simple storage service. Amazon S3 is an **object level storage** that cannot be used to store running operating systems or live databases.

"Amazon EFS" is incorrect. Amazon EFS refers to the Amazon Elastic File System. Amazon EFS is a file level storage that provides a scalable, elastic **NFS file system** for Linux-based workloads for use with AWS Cloud services and on-premises resources. Amazon RDS does not use Amazon EFS to store databases.

"Amazon Glacier" is incorrect. Amazon Glacier is used for storing backups and long-term data.

References:

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

Question 32: **Incorrect**

What are the change management tools that helps AWS customers audit and monitor all resource changes in their AWS environment? (Choose TWO)

-

Amazon Comprehend

(Incorrect)

-

AWS CloudTrail

(Correct)

-

AWS Config

(Correct)

-

AWS X-Ray

(Incorrect)

-

AWS Transit Gateway

Explanation

Change management is defined as "the Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT Services.

Despite all of the investments in software and hardware, an erroneous configuration or misstep in a process can frequently undo these efforts and lead to failure.

AWS Config and AWS CloudTrail are change management tools that help AWS customers audit and monitor all resource and configuration changes in their AWS environment

Customers can use AWS Config to answer "What did my AWS resource look like?" at a point in time. Customers can use AWS CloudTrail to answer "Who made an API call to modify this resource?" For example, a customer can use the AWS Management Console for AWS Config to detect that the security group "Production-DB" was incorrectly configured in the past. Using the integrated AWS CloudTrail information, they can pinpoint which user misconfigured the "Production-DB" security group. In brief, AWS Config provides information about the changes made to a resource, and AWS CloudTrail provides information about who made those

changes. These capabilities enable customers to discover any misconfigurations, fix them, and protect their workloads from failures.

The other options are incorrect:

"AWS Transit Gateway" is incorrect. AWS Transit Gateway is a network transit hub that customers can use to interconnect their virtual private clouds (VPCs) and their on-premises networks. AWS transit gateway simplifies how customers interconnect all of their VPCs, across thousands of AWS accounts and into their on-premises networks.

"AWS X-Ray" is incorrect. AWS X-Ray is a debugging service that helps developers understand how their application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.

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

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

References:

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

Question 33: **Incorrect**

Your company is designing a new application that will store and retrieve photos and videos. Which of the following services should you recommend as the underlying storage mechanism?

- Amazon EBS
(Incorrect)
- Amazon S3
(Correct)
- Amazon SQS
- Amazon Instance store

Explanation

Amazon S3 is object storage built to store and retrieve any amount of data from anywhere on the Internet. It is a storage service that offers an extremely durable, highly available, and infinitely scalable data storage infrastructure at very low costs.

Common use cases of Amazon S3 include:

Media Hosting – Build a redundant, scalable, and highly available infrastructure that hosts video, photo, or music uploads and downloads.

Backup and Storage – Provide data backup and storage services for others.

Hosting static websites – Host and manage static websites quickly and easily.

Deliver content globally - Use S3 in conjunction with CloudFront to distribute content globally with low latency.

Hybrid cloud storage - Create a seamless connection between on-premises applications and Amazon S3 with **AWS Storage Gateway** in order to reduce your data center footprint, and leverage the scale, reliability, and durability of AWS.

The other options are incorrect:

"Amazon SQS" is incorrect. Amazon SQS is not a storage service. It is a messaging queuing service that can be used to send messages between application components. SQS enables you to decouple and scale microservices, distributed systems, and serverless applications.

"Amazon Instance store" is incorrect. Amazon EC2 Instance Store provides temporary block-level storage for your instance. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.

"Amazon EBS" is incorrect. Amazon EBS is not a cost-effective solution for storing images or videos (compared to Amazon S3). Amazon EBS is a block level storage that can be used as a disk drive for Amazon EC2 or Amazon RDS instances. Amazon EBS is designed for application workloads that benefit from fine tuning for performance and capacity. Typical use cases of Amazon EBS include Big Data analytics engines (like the Hadoop/HDFS ecosystem and Amazon EMR clusters), relational and NoSQL databases (like Microsoft SQL Server and MySQL or Cassandra and MongoDB), stream and log processing applications (like Kafka and Splunk), and data warehousing applications (like Vertica and Teradata).

References:

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

Question 34: **Incorrect**

What is the AWS data warehouse service that supports a high level of query performance on large amounts of datasets?

-

Amazon Redshift

(Correct)

-

Amazon Kinesis

-

Amazon DynamoDB

(Incorrect)



Amazon RDS

Explanation

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. It allows you to run complex analytic queries against petabytes of structured data. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. Amazon Redshift manages the work needed to set up, operate, and scale a data warehouse, from provisioning the infrastructure capacity to automating ongoing administrative tasks such as backups, and patching.

The other options are incorrect:

"Amazon Kinesis" is incorrect. Amazon Kinesis is used to collect, process, and analyze video and data streams in real time.

"Amazon RDS" is incorrect. Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the AWS Cloud. Amazon RDS provides you with **six relational database engines** to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and Microsoft SQL Server.

"Amazon DynamoDB" is incorrect. Amazon DynamoDB is a NoSQL database service.

References:

<https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html>

Question 35: **Incorrect**

A company is developing a new application using a microservices framework. The new application is having performance and latency issues. Which AWS Service should be used to troubleshoot these issues?

- Amazon Inspector

(Incorrect)

- AWS CloudTrail
- AWS CodePipeline
- AWS X-Ray

(Correct)

Explanation

AWS X-Ray helps developers analyze and debug distributed applications in production or under development, such as those built using microservice architecture. With X-Ray, you can understand how your application and its underlying services are performing so you can identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components. You can use X-Ray to analyze both applications in development and in production, from simple three-tier applications to complex microservices applications consisting of thousands of services.

The other options are incorrect:

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

"AWS Inspector" is incorrect. Amazon Inspector helps you to identify security vulnerabilities as well as deviations from security best practices in applications NOT for troubleshooting performance issues.

"AWS CloudTrail" is incorrect. CloudTrail is a service that allows you to track all users' actions that are taken in your AWS account.

References:

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

Question 36: **Correct**

Which of the following is equivalent to a user name and password and is used to authenticate your programmatic access to AWS services and APIs?



Access Keys

(Correct)



Key pairs



Instance Password



MFA

Explanation

Access keys consist of two parts: an access key ID and a secret access key. You must provide your AWS access keys to make programmatic requests to AWS or to use the AWS Command Line Interface or AWS Tools for PowerShell. Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests.

The other options are incorrect:

"MFA" is incorrect. MFA is an additional security layer that can be used to secure your AWS console. MFA can also be used to control access to AWS service APIs.

"Instance Password" is incorrect. There are no passwords related to the EC2 instances.

"Key pairs" is incorrect. The AWS key pair is used to securely connect to your Amazon EC2 instances.

References:

<https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

Question 37: **Incorrect**

Which of the following should be considered when performing a TCO analysis to compare the costs of running an application on AWS instead of on-premises?

- Market research
- Business analysis

(Incorrect)

- Application development
- Physical hardware

(Correct)

Explanation

Weighing the financial considerations of owning and operating a data center facility versus employing a cloud infrastructure requires detailed and careful analysis. The Total Cost of Ownership (TCO) is often the financial metric used to estimate and compare costs of a product or a service. When comparing AWS with on-premises TCO, customers should consider all costs of owning and operating a data center. Examples of these costs include facilities, physical servers, storage devices, networking equipment, cooling and power consumption, data center space, and Labor IT cost.

The other options are incorrect.

"Application development" is incorrect. Application development is the process of creating a program or a set of programs to perform the different tasks that a business requires. Application development is a separate process that customers need to perform regardless of whether they will be using AWS or an on-premises data center. Application development is not part of the total cost of owning and operating a data center (TCO), and thus is an incorrect answer.

"Market Research" is incorrect. Market research is an organized effort to gather information about target audience and customers to determine how viable a product or service might be. Market research is a separate process that customers need to perform regardless of whether they will be using AWS or an on-premises data center.

"Business analysis" is incorrect. Business analysis is a multistage process aimed at identifying business needs and determining solutions to business problems. Business analysis is a separate process that customers need to perform regardless of whether they will be using AWS or an on-premises data center.

References:

<https://aws.amazon.com/blogs/publicsector/cloud-economics-value-tco-assessment/>

Question 38: **Correct**

Which of the following services can help protect your web applications from SQL injection and other vulnerabilities in your application code?

- AWS IAM
- AWS WAF
- Amazon Cognito
- Amazon Aurora

Explanation

AWS WAF (Web Application Firewall) helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.

The other options are incorrect:

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

"AWS IAM" is incorrect. AWS IAM refers to the AWS Identity and Access Management.

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

References:

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

Question 39: **Incorrect**

Amazon Glacier is an Amazon S3 storage class that is suitable for storing _____ & _____. (Choose TWO)

- Dynamic websites' assets
- Cached data

(Incorrect)

- Active databases
- Long-term analytic data

(Correct)

- Active archives

(Correct)

Explanation

Amazon S3 Glacier provides three retrieval options to fit your use case. Expedited retrievals typically return data in 1-5 minutes, and are best used for Active Archive use cases. Standard retrievals typically complete between 3-5 hours work, and work well for less time-sensitive needs like backup data, media editing, or long-term analytics. Bulk retrievals are the lowest-cost retrieval option, returning large amounts of data within 5-12 hours.

The other options are incorrect:

"Active databases" is incorrect. Active databases require consistent and low-latency storage performance. For example, DB instances for Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server use Amazon Elastic Block Store (Amazon EBS) volumes for database and log storage.

"Cached data" is incorrect. A cache is a high-speed data storage layer which stores a subset of data, typically transient in nature, so that future requests for that data are served up faster than is possible by accessing the data's primary storage location. Caching allows you to efficiently reuse previously retrieved or computed data. The data in a cache is generally stored in fast access hardware such as RAM (Random-access memory) and may also be used in correlation with a software component. A cache's primary purpose is to increase data retrieval performance by reducing the need to access the underlying slower storage layer.

"Dynamic websites' assets" is incorrect. Dynamic websites usually require immediate retrieval, which is not available in Glacier.

References:

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

Question 40: **Correct**

A company has a large amount of structured data stored in their on-premises data center. They are planning to migrate all the data to AWS, what is the most appropriate AWS database option?



Amazon RDS

(Correct)



Amazon SNS



Amazon DynamoDB

• ○

Amazon ElastiCache

Explanation

Since the data is **structured**, then it is best to use a relational database service such as Amazon RDS.

The other options are incorrect:

"Amazon ElastiCache" is incorrect. ElastiCache is an in-memory data store and cache service.

"Amazon DynamoDB" is incorrect. DynamoDB is a NoSQL database service. NoSQL is designed for **unstructured** data.

"Amazon SNS" is incorrect. Amazon Simple Notification Service (SNS) is not a database service. Amazon SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

References:

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

Question 41: **Incorrect**

What does Amazon Elastic Beanstalk provide?

- ○

A scalable file storage solution for use with AWS and on-premises servers

- ○

A PaaS solution to automate application deployment

(Correct)

- A NoSQL database service

(Incorrect)

- A compute engine for Amazon ECS

Explanation

AWS Elastic Beanstalk is an application container on top of Amazon Web Services. Elastic Beanstalk makes it easy for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application code, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

The other options are incorrect. AWS Elastic Beanstalk is not a database, compute engine nor storage service, AWS Elastic Beanstalk uses proven AWS features and services, such as Amazon EC2, Amazon RDS, Elastic Load Balancing, Auto Scaling, Amazon S3, and Amazon SNS, to create an environment that runs your application.

References:

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

Question 42: **Incorrect**

Using Amazon RDS falls under the shared responsibility model. Which of the following are customer responsibilities? (Choose TWO)

-

Performing backups

-

Managing the database settings

(Correct)

-

Patching the database software

(Incorrect)

-

Building the relational database schema

(Correct)

-

Installing the database software

Explanation

Amazon RDS manages the work involved in setting up a relational database, from provisioning the infrastructure capacity you request to installing the database software. Once your database is up and running, Amazon RDS automates common administrative tasks such as performing backups and patching the software that powers your database. With optional Multi-AZ deployments, Amazon RDS also manages synchronous data replication across Availability Zones with automatic failover. Since Amazon RDS provides native database access, you interact with the relational database software as you normally would. This means you're still responsible for managing the database settings that are specific to your application. You'll need to build the relational schema that best fits your use case and are responsible for any performance tuning to optimize your database for your application's workflow.

The other options are incorrect:

"Installing the database software" is incorrect. Installing the database software is AWS' responsibility.

"Performing backups" is incorrect. Performing backups is AWS' responsibility.

"Patching the database software" is incorrect. Patching the database software is AWS' responsibility.

References:

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

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

Question 43: Correct

What is the AWS service that enables you to manage all of your AWS accounts from a single master account?

- AWS WAF
- AWS Trusted Advisor
- Amazon Config
- AWS Organizations

(Correct)

Explanation

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.

AWS Organizations enables the following capabilities:

- 1- Automate AWS account creation and management
- 2- Consolidate billing across multiple AWS accounts
- 3- Govern access to AWS services, resources, and regions
- 4- Centrally manage access policies across multiple AWS accounts
- 5- Configure AWS services across multiple accounts

The other options are incorrect:

"AWS Trusted Advisor" is incorrect. 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).**

"Amazon Config" is incorrect. Amazon Config is used to record and evaluate configurations of your AWS resources.

"AWS WAF" is incorrect. AWS WAF is a AWS web application firewall that helps protect your web applications.

References:

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

Question 44: **Correct**

What are the AWS services\features that can help you maintain a highly available and fault-tolerant architecture in AWS? (Choose TWO)

-

Network ACLs

-

CloudFormation

-

Amazon EC2 Auto Scaling

(Correct)

-

Elastic Load Balancer

(Correct)

-

AWS Direct Connect

Explanation

Amazon EC2 Auto Scaling is a fully managed service designed to launch or terminate Amazon EC2 instances automatically to help ensure you have the correct number of Amazon EC2 instances available to handle the load for your application. Amazon EC2 Auto Scaling helps you maintain application availability and fault tolerance through fleet management for EC2 instances, which detects and replaces unhealthy instances, and by scaling your Amazon EC2 capacity automatically according to conditions you define. You can use Amazon EC2 Auto Scaling to automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.

Elastic Load Balancing provides an effective way to increase the availability and fault tolerance of a system. First ELB tries to discover the availability of your EC2 instances, it periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called health checks. The load balancer routes user requests only to the healthy instances. When the load balancer determines that an instance is unhealthy, it stops routing requests to that instance. The load balancer resumes routing requests to the instance when it has been restored to a healthy state.

The other options are incorrect:

"CloudFormation" is incorrect. AWS CloudFormation automates and simplifies the task of creating groups of related resources that power your applications. 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.

"Network ACLs" is incorrect. Network ACLs is used to control traffic at the subnet level.

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

References:

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

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

Question 45: Incorrect

Which of the following AWS security features is associated with an EC2 instance and functions to filter incoming traffic requests?

- Security Groups
- **(Correct)**
- AWS Systems Manager Session Manager
- VPC Flow logs
- Network ACL

(Incorrect)

Explanation

Security Groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

The following table summarizes the basic differences between security groups and network ACLs.

Security group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets that it's associated with (therefore, it provides an additional layer of defense if the security group rules are too permissive)

Via -

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison

The other options are incorrect:

"Network ACL" is incorrect. A network access control list (Network ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

Note: Network ACLs act at the subnet level, but security groups act at the instance level.

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

"VPC Flow logs" is incorrect. The VPC Flow logs feature does not filter traffic. You can use security groups to filter traffic at the instance level and Network ACLs to filter traffic at the subnet level. VPC Flow logs only **capture information** about the IP traffic going to and from network interfaces in your VPC. This information can help

you **monitor the traffic** that is reaching your instances and diagnose overly restrictive or overly permissive security group and network ACL rules.

AWS customers use VPC Flow logs to **troubleshoot connectivity and security issues** and make sure that network access rules are working as expected.

Security Groups, Network ACLs, and VPC Flow logs are advanced topics, but they are required for the Cloud Practitioner exam! If you understand what we've mentioned above, you should be able to answer any questions related to these topics.

References:

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

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

Question 46: **Incorrect**

Which of the following AWS offerings is a MySQL-compatible relational database service that can scale capacity automatically based on demand?

-

Amazon Neptune

(Incorrect)

-

Amazon RDS for PostgreSQL

-

Amazon RDS for SQL Server

-

Amazon Aurora

(Correct)

Explanation

Amazon Aurora is a MySQL and PostgreSQL compatible relational database built for the cloud, that combines the performance and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases. Aurora is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases. It provides the security, availability, and reliability of commercial-grade databases at 1/10th the cost. Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.

Amazon Aurora features "Amazon Aurora Serverless" which is an on-demand, auto-scaling configuration for Amazon Aurora (MySQL-compatible and PostgreSQL-compatible editions), where the database will automatically start up, shut down, and scale capacity up or down based on your application's needs.

The other options are incorrect:

"Amazon RDS PostgreSQL" is incorrect. Amazon RDS PostgreSQL is used to run PostgreSQL databases NOT MySQL databases.

"Amazon RDS for SQL Server " is incorrect. Amazon RDS for SQL Server is used to run Microsoft SQL Server databases NOT MySQL databases.

"Amazon Neptune" is incorrect. Amazon Neptune is a graph database service NOT a MySQL database. Amazon Neptune can be 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 47: **Incorrect**

Under the Shared Responsibility Model, which of the following controls do customers fully inherit from AWS? (Choose TWO)

- Awareness & Training
- Database controls
(Incorrect)
- Patch management controls
(Incorrect)
- Physical controls
(Correct)
- Environmental controls
(Correct)

Explanation

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

As mentioned in the [AWS Shared Responsibility Model page](#), Inherited Controls are controls which a customer fully inherits from AWS such as physical controls and environmental controls.

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

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

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

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

The other options are incorrect:

"Patch management controls" is incorrect. Patch Management belongs to the shared controls. 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.

"Database controls" is incorrect. Database controls belongs to the shared controls. AWS maintains the configuration of its infrastructure devices that run the database, but customers are responsible for configuring their own databases, and applications.

"Awareness & Training" is incorrect. Awareness & Training belongs to the shared controls. AWS trains AWS employees, but customers must train their own employees.

References:

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

Question 48: Incorrect

A company has created a solution that helps AWS customers improve their architectures on AWS. Which AWS program may support this company?

- APN Consulting Partners
(Correct)
- APN Technology Partners
- AWS TAM
- AWS Professional Services
(Incorrect)

Explanation

APN 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. AWS supports the APN Consulting Partners by providing a wide range of resources and training to support their customers.

The other options are incorrect:

"APN Technology Partners" is incorrect. APN Technology Partners provide software solutions that are either hosted on, or integrated with, the AWS platform. APN Technology Partners include Independent Software Vendors (ISVs), SaaS, PaaS, Developer Tools, Management and Security Vendors.

"AWS Professional Services" is incorrect. AWS Professional Services shares a collection of offerings to help you achieve specific outcomes related to enterprise cloud adoption. AWS Professional Services also trains your team with specialized skills and provides global specialty practices to support your efforts in focused areas of enterprise cloud computing.

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

References:

<https://aws.amazon.com/partners/consulting/>

<https://d1.awsstatic.com/whitepapers/aws-partners-customers-work-together-website.pdf>

Question 49: **Correct**

What is the AWS service that performs automated network assessments of Amazon EC2 instances to check for vulnerabilities?

- Security groups
- Amazon Inspector
- Amazon Kinesis
- AWS Network Access Control Lists

Explanation

Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to create assessment templates to automate security vulnerability assessments throughout your development and deployment pipelines or for static production systems.

The other options are incorrect:

"Security groups" is incorrect. Security groups can be used to check the network accessibility of your Amazon EC2 instances -at the instance level- but this is not done automatically.

"Amazon Kinesis" is incorrect. Amazon Kinesis allows you to collect, process, and analyze video and data streams in real time.

"AWS Network Access Control Lists" is incorrect. AWS Network Access Control Lists can be used to check the network accessibility of your Amazon EC2 instances -at the subnet level- but this is not done automatically.

References:

https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html

Question 50: **Incorrect**

What are the Amazon RDS features that can be used to improve the availability of your database? (Choose TWO)

-

Edge Locations

(Incorrect)

-

Read Replicas

(Correct)

-

Multi-AZ Deployment

(Correct)

-

AWS Regions

(Incorrect)

-

Automatic patching

Explanation

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput.

Read replicas provide a complementary availability mechanism to Amazon RDS Multi-AZ Deployments. You can promote a read replica if the source DB instance fails. You can also replicate DB instances across AWS Regions as part of your disaster recovery strategy. This functionality complements the synchronous replication, automatic failure detection, and failover provided with Multi-AZ deployments.

The other options are incorrect:

"Edge Locations" is incorrect. Edge Locations are not a feature of Amazon RDS. Edge locations are used by the CloudFront service to distribute content globally.

"Automatic patching" is incorrect. The purpose of patching is to resolve functionality issues, improve security or add new features.

"AWS Regions" is incorrect. AWS Regions are not a feature of Amazon RDS. AWS Regions are separate geographic areas around the world that AWS uses to provide its Cloud Services, including Regions in North America, South America, Europe, Asia Pacific, and the Middle East. Choosing a specific AWS Region depends on its proximity to end-users, data sovereignty, and costs.

References:

<https://aws.amazon.com/rds/details/multi-az/>

<https://aws.amazon.com/rds/details/read-relicas/>

Question 51: **Incorrect**

What is the AWS service that provides you the highest level of control over the underlying virtual infrastructure?

- Amazon RDS
- Amazon Redshift
- (Incorrect)
- Amazon DynamoDB
- Amazon EC2

(Correct)

Explanation

Amazon EC2 provides you the highest level of control over your virtual instances, including root access and the ability to interact with them as you would any machine.

The other options are incorrect:

Amazon DynamoDB, Amazon RDS, and Amazon Redshift belong to the AWS-managed services. The AWS-managed services automate time-consuming administration tasks such as hardware provisioning, software 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.

References:

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

Question 52: **Incorrect**

What are two advantages of using Cloud Computing over using traditional data centers? (Choose TWO)

-

Virtualized compute resources

(Incorrect)

-

Distributed infrastructure

(Correct)

-

Dedicated hosting

-

Reserved Compute capacity

-

Eliminating Single Points of Failure (SPOFs)

(Correct)

Explanation

These are things that traditional web hosting cannot provide:

****High-availability (eliminating single points of failure):** A system is highly available when it can withstand the failure of an individual component or multiple components, such as hard disks, servers, and network links. The best way to understand and avoid the single point of failure is to begin by making a list of all major points of your architecture. You need to break the points down and understand them further. Then, review each of these points and think what would happen if any of these failed. AWS gives you the opportunity to automate recovery and reduce disruption at every layer of your architecture.

Additionally, AWS provides fully managed services that enable customers to offload the administrative burdens of operating and scaling the infrastructure to AWS so that they don't have to worry about high availability or Single Point of Failures. For example, AWS Lambda and DynamoDB are serverless services; there are no servers to provision, patch, or manage and no software to install, maintain, or operate. Availability and fault tolerance are built-in, eliminating the need to architect your applications for these capabilities.

****Distributed infrastructure:** The AWS Cloud operates in over 75 Availability Zones within over 20 geographic Regions around the world, with announced plans for more Availability Zones and Regions, allowing you to reduce latency to users from all around the world.

****On-demand infrastructure for scaling applications or tasks:** AWS allows you to provision the required resources for your application in minutes and also allows you to stop them when you don't need them.

****Cost savings:** You don't have to run your own data center for internal or private servers, so your IT department doesn't have to make bulk purchases of servers which may never get used, or may be inadequate. The "pay as you go" model from AWS allows you to pay only for what you use and the ability to scale down to avoid overspending. With AWS you don't have to pay an entire IT department to maintain that hardware -- you don't even have to pay an accountant to figure out how much hardware you can afford or how much you need to purchase.

The other options are incorrect. Both cloud computing and traditional data centers can provide virtualized compute resources, dedicated hosting and reserved Compute capacity.

References:

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

Question 53: **Incorrect**

A company has business critical workloads hosted on AWS and they are unwilling to accept any downtime. Which of the following is a recommended best practice to protect their workloads in the event of an unexpected natural disaster?

- Deploy AWS resources across multiple Availability Zones within the same AWS Region

(Incorrect)

- Replicate data across multiple Edge Locations worldwide and use Amazon CloudFront to perform automatic failover in the event of an outage
- Deploy AWS resources to another AWS Region and implement an Active-Active disaster recovery strategy

(Correct)

- Create point-in-time backups in another subnet and recover this data when a disaster occurs

Explanation

Disaster recovery is about preparing for and recovering from events that have a negative impact on your business continuity or finances. This could be a natural disaster, hardware or software failure, a network outage, a power outage, physical damage to a building like fire or flooding, or some other significant disaster.

In AWS, customers have the flexibility to choose the disaster recovery approach that fits their budget. The approaches could be as minimum as backup and restore from another AWS Region or full-scale multi-region Active-Active solution.

With the multi-region Active-Active solution, your workload is deployed to, and actively serving traffic from, multiple AWS Regions. If an entire Region goes down because of a natural disaster or any other reason, the other Regions will still be available and able to serve user requests.

The other options are incorrect:

"Deploy AWS resources across multiple Availability Zones within the same AWS Region" is incorrect. A natural disaster may affect an entire Region, including all Availability Zones within that Region.

"Replicate data across multiple Edge Locations worldwide and use Amazon CloudFront to perform automatic failover in the event of an outage" is incorrect. Edge locations are not used for disaster recovery. Edge locations are used by CloudFront to cache and distribute content from a geographical location close to users.

"Create point-in-time backups in another subnet and recover this data when a disaster occurs" is incorrect. A subnet is a range of IP addresses within a VPC.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/wellarchitected-reliability-pillar.pdf#plan-for-disaster-recovery-dr>

Question 54: **Incorrect**

Which of the following will impact the price paid for an EC2 instance? (Choose TWO)

-

Number of private IPs

(Incorrect)

-

The Availability Zone where the instance is provisioned

(Incorrect)

-

Load balancing

(Correct)

-

Number of buckets

-

Instance type

(Correct)

Explanation

EC2 instance pricing varies depending on many variables:

- The buying option (On-demand, Savings Plans, Reserved, Spot, Dedicated)
- Selected instance type
- Selected Region
- Number of instances
- Load balancing
- Allocated Elastic IP Addresses

Load balancing: The number of hours the Elastic Load Balancer runs and the amount of data it processes contribute to the EC2 monthly cost.

Instance type: Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity.

The other options are incorrect:

"The Availability Zone where the instance is provisioned" is incorrect. Prices of the Amazon EC2 instances may vary depending on the Region where the instances are provisioned. Amazon EC2 instances provisioned in different Availability Zones within the same Region have the same price.

"Number of private IPs" is incorrect. There is no charge for private IPs.

Additional information:

The number of allocated Elastic IPs is the factor that may affect Amazon EC2 charges. To ensure efficient use of Elastic IP addresses, AWS imposes a small hourly charge if an Elastic IP address is **not associated** with a running instance, or if it is **associated** with a stopped instance. While the instance is running, you are not charged for one Elastic IP address associated with the instance, but additional Elastic IPs are not free.

"Number of buckets" is incorrect. A bucket is an Amazon S3 resource, not an Amazon EC2 resource.

Additional information:

To upload your data (photos, videos, documents, etc.) to Amazon S3, you must first create an S3 bucket (which is like a file folder) in one of the AWS Regions. You can then upload any number of objects to the bucket. The customer is charged based on the total size of the objects (in GB) stored in their S3 bucket, not for the bucket itself.

References:

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

Question 55: **Correct**

Jessica is managing an e-commerce web application in AWS. The application is hosted on six EC2 instances. One day, three of the instances crashed; but none of her customers were affected. What has Jessica done correctly in this scenario?

-

She has properly built a fault tolerant system

(Correct)

-

She has properly built an encrypted system

-

She has properly built a scalable system

-

She has properly built an elastic system

Explanation

Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of some (one or more faults within) of its components. Visitors to a website expect the website to be available irrespective of when they visit. For example, when someone wants to visit Jessica's website to purchase a product, whether it is at 9:00 AM on a Monday or 3:00 PM on holiday, he\she expects that the website will be available and ready to accept his\her purchase. Failing to meet these expectations can cause loss of business and contribute to the development of a negative reputation for the website owner, resulting in lost revenue.

The other options are incorrect:

"She has properly built an elastic system" is incorrect. Elasticity is the ability of a system to scale the resources needed to cope with load dynamically. So that when

the load increases you scale by adding more resources and when demand wanes you shrink back and remove unneeded resources.

"She has properly built a scalable system" is incorrect. Scalability is the ability of a system to accommodate larger loads just by adding resources, either making hardware larger (scaling vertically) or adding additional nodes (scaling horizontally).

"She has properly built an encrypted system" is incorrect. Encryption is much more related to data protection, not fault-tolerance.

References:

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

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.scalability.en.html>

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html>

Question 56: **Correct**

Where can you store files in AWS? (Choose TWO)

-

Amazon EFS

(Correct)

-

Amazon EMR

-

Amazon SNS

-

Amazon ECS

-

Amazon EBS

(Correct)

Explanation

** Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It is easy to use and offers a simple interface that allows you to create and configure file systems quickly and easily. Amazon EFS is built to elastically scale on demand without disrupting applications, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it. It is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS that scale as a file system grows, with consistent low latencies. As a regional service, Amazon EFS is designed for high availability and durability storing data redundantly across multiple Availability Zones.

** Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability.

The other options are incorrect:

"Amazon SNS" is incorrect. Amazon Simple Notification Service (SNS) is a pub/sub messaging service.

"Amazon ECS" is incorrect. Amazon Elastic Container Service (ECS) is a compute service that is used to run containerized applications on AWS.

"Amazon EMR" is incorrect. Amazon Elastic MapReduce (EMR) is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-

effectively process vast amounts of data across dynamically scalable Amazon EC2 instances.

References:

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

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

Question 57: **Incorrect**

What are the connectivity options that can be used to build hybrid cloud architectures? (Choose TWO)

- AWS VPN
- **(Correct)** AWS CloudTrail
- AWS Direct Connect
- **(Correct)** AWS Artifact
- AWS Cloud9

Explanation

In cloud computing, hybrid cloud refers to the use of both on-premises resources in addition to public cloud resources. A hybrid cloud enables an organization to migrate applications and data to the cloud, extend their datacenter capacity, utilize new cloud-native capabilities, move applications closer to customers, and create a backup and disaster recovery solution with cost-effective high availability. By working closely with enterprises, AWS has developed the industry's broadest set of hybrid capabilities across storage, networking, security, application

deployment, and management tools to make it easy for you to integrate the cloud as a seamless and secure extension of your existing investments.

AWS Virtual Private Network solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network. 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. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your on-premises network or branch office site and Amazon VPC. AWS Direct Connect is a network service that provides an alternative to using the Internet to connect customer's on-premise sites to AWS. Using AWS Direct Connect, data that would have previously been transported over the Internet can now be delivered through a private network connection between AWS and your datacenter or corporate network. Companies of all sizes use AWS Direct Connect to establish private connectivity between AWS and datacenters, offices, or colocation environments. **Compared to AWS VPN (Internet-based connection), AWS Direct Connect can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience.**

Additional information:

Besides the connectivity options that AWS provides, AWS provides many features to support building more efficient hybrid cloud architectures. For example, AWS Identity and Access Management (IAM) can grant your employees and applications access to the AWS Management Console and AWS service APIs using your existing corporate identity systems. AWS IAM supports federation from corporate systems like Microsoft Active Directory, as well as external Web Identity Providers like Google and Facebook.

The other options are incorrect:

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

"AWS Artifact" is incorrect. AWS Artifact provides on-demand access to AWS' compliance reports.

"AWS CloudTrail" is incorrect. AWS CloudTrail is a web service that tracks and records all user interactions with AWS services.

References:

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

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

Question 58: **Incorrect**

Which of the following AWS services is designed with native Multi-AZ fault tolerance in mind? (Choose TWO)

-

AWS Snowball

(Incorrect)

-

Amazon EBS

-

Amazon Simple Storage Service

(Correct)

-

Amazon Redshift

-

Amazon DynamoDB

(Correct)

Explanation

The Multi-AZ principle involves deploying an AWS resource in multiple Availability Zones to achieve high availability for that resource.

DynamoDB automatically spreads the data and traffic for your tables over a sufficient number of servers to handle your throughput and storage requirements, while maintaining consistent and fast performance. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in fault tolerance in the event of a server failure or Availability Zone outage.

Amazon S3 provides durable infrastructure to store important data and is designed for durability of 99.999999999% of objects. Data in all Amazon S3 storage classes is redundantly stored across multiple Availability Zones (except S3 One Zone-IA).

The other options are incorrect:

"Amazon Redshift" is incorrect. Currently, Amazon Redshift only supports Single-AZ deployments.

"AWS Snowball" is incorrect. AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS using storage devices designed to be secure for physical transport.

"Amazon EBS" is incorrect. Amazon EBS volume data is replicated across multiple servers within the same Availability Zone.

Note:

Amazon EFS data is redundantly stored across multiple Availability Zones providing better durability compared to EBS volumes.

References:

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

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

Question 59: **Incorrect**

How are AWS customers billed for Linux-based Amazon EC2 usage?

- EC2 instances will be billed on one day increments, with a minimum of one month
- EC2 instances will be billed on one second increments, with a minimum of one minute

(Correct)

- EC2 instances will be billed on one minute increments, with a minimum of one hour

(Incorrect)

- EC2 instances will be billed on one hour increments, with a minimum of one day

Explanation

Pricing is per instance-hour consumed for each instance, from the time an instance is launched until it is terminated or stopped. Each partial instance-hour consumed will be billed per-second (minimum of 1 minute) for Linux, Windows, or Ubuntu Instances and as a full hour for all other instance types.

Examples for Linux, Windows, or Ubuntu based instances:

1- If you run a Linux instance for 4 seconds or 20 seconds or 59 seconds, you will be charged for one minute. (this is what we mean by minimum of 1 minute)

2- If you run a Linux instance for 1 minute and 3 seconds, you will be charged for 1 minute and 3 seconds.

3- If you run a Linux instance for 3 hours, 25 minutes and 7 seconds, you will be charged for 3 hours, 25 minutes and 7 seconds.

Examples for instances launched in other operating systems such as Red Hat, Kali, or CentOS:

1- If you run an instance for 4 seconds or 20 seconds or 59 seconds, you will be charged for one hour.

2- If you run an instance for 1 minute and 3 seconds, you will be charged for one hour.

3- If you run an instance for 3 hours, 25 minutes and 7 seconds, you will be charged for 4 hours.

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 60: **Correct**

Which of the following describes the payment model that AWS makes available for customers that can commit to using Amazon EC2 over a one or 3-year term to reduce their total computing costs?



Pay as you go



Pay less by using more



Save when you reserve

(Correct)



Pay less as AWS grows

Explanation

For Customers that can commit to using EC2 over a 1 or 3-year term, it is better to use Amazon EC2 Reserved Instances. Reserved Instances provide a significant discount (up to 75%) compared to On-Demand instance pricing.

The other options are incorrect:

"Pay as you go" is incorrect. Reserved Instances provide a significant discount (up to 75%) compared to On-Demand (pay-as-you-go) instance pricing.

"Pay less as AWS grows" is incorrect. Pay less as AWS grows refers to the discounts that you get over time as AWS grows. This sometimes called "AWS Economies of Scale". For example, AWS has reduced the per GB storage price of S3 by 80% since the service was first introduced in 2006.

"Pay less by using more" is incorrect. "Pay less by using more" means that you get volume based discounts and as your usage increases. For services such as S3, pricing is tiered, meaning the more you use, the less you pay per GB.

References:

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

Question 61: **Incorrect**

Your application has recently experienced significant global growth, and international users are complaining of high latency. What is the AWS characteristic that can help improve your international users' experience?

-
- Data durability
-
- Elasticity

(Incorrect)

-
- High availability
-
- Global reach

(Correct)

Explanation

With AWS, you can deploy your application in multiple regions around the world. The user will be redirected to the Region that provides the lowest possible latency and the highest performance. You can also use the CloudFront service that uses edge locations (which are located in most of the major cities across the world) to deliver content with low latency and high performance to your global users.

The other options are incorrect:

"High availability" is incorrect. High Availability can be achieved by deploying your application in multiple Availability Zones within a single Region. If one Availability Zone goes down, the others can handle user requests. This may not reduce latency to your international users. In other words, the application will be available for them all the time, but with high latency.

"Elasticity" is incorrect. Elasticity refers to the ability of a system to scale the underlying resources up when demand increases (to maintain performance), or scale down when demand decreases (to reduce costs). This option does not indicate whether your resources will be deployed in a single Region or multiple Regions.

"Data durability" is incorrect. Durability refers to the ability of a system to assure data is stored and data remains consistent in the system as long as it is not changed by legitimate access. This means that data should not become corrupted or disappear due to a system malfunction. Durability is used to measure the likelihood of data loss. For example, assume you have confidential data stored in your Laptop. If you make a copy of it and store it in a secure place, you have just improved the durability of that data. It is much less likely that all copies will be simultaneously destroyed.

Data durability can be achieved by replicating data across multiple Availability Zones within a single Region. For example, the S3 Standard Tier is designed for 99.99999999% durability. This means that if you store 100 billion objects in S3, you will lose one object at most.

References:

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

Question 62: **Correct**

Which AWS services can be used to improve the performance of a global application and reduce latency for its users? (Choose TWO)

- AWS KMS
- AWS Glue
- AWS Direct Connect
- AWS Global accelerator

(Correct)

-

Amazon CloudFront

(Correct)

Explanation

AWS Global Accelerator and CloudFront are two separate services that use the AWS global network and its edge locations around the world. Amazon CloudFront improves performance for global applications by caching content at the closest Edge Location to end-users. AWS Global Accelerator improves performance for global applications by routing end-user requests to the closest AWS Region. Amazon 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.

Note: AWS Global accelerator does not cache content at edge locations like Amazon CloudFront. AWS Global accelerator uses the AWS edge locations to receive end-user requests and then routes these requests to the closest AWS Region over the AWS global network.

The other options are incorrect:

"AWS KMS" is incorrect. AWS KMS is a key management service that makes it easy for you to create and manage encryption keys and control their use across a wide range of AWS services and in your applications.

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

"AWS Glue" is incorrect. AWS Glue is a fully-managed, Extract, Transform, and Load (ETL) service that automates the time-consuming steps of data preparation for analytics.

Extract, Transform, and Load (ETL) is the process of **extracting** (collecting) data from various sources (from different databases for example), **transform** the data depending on business rules/needs (This step helps in preparing the data for analytics and decision making) and **load** the data into a destination database, often a data warehouse.

References:

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

<https://aws.amazon.com/global-accelerator/features/>

Question 63: **Incorrect**

Which of the following procedures will help reduce your Amazon S3 costs?

- Move all the data stored in S3 standard to EBS
- Pick the right Availability Zone for your S3 bucket
- Use the Import/Export feature to move old files automatically to Amazon Glacier
- **(Incorrect)**
- **(Correct)** Use the right combination of storage classes based on different use cases

Explanation

Amazon S3 offers a range of storage classes designed for different use cases. These include S3 Standard for general-purpose storage of frequently accessed data; S3 Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation.

The other options are incorrect:

"Move all the data stored in S3 standard to EBS" is incorrect. EBS is a block-level storage service that is significantly more expensive than S3.

"Pick the right Availability Zone for your S3 bucket" is incorrect. You don't have the option to store objects on a specific AZ. You can only choose the AWS Region in which you want your S3 buckets to reside.

Additional information:

In general, AWS prices for a resource may change based on the AWS Region where it is created, NOT based on Availability Zones within the same Region.

"Use the Import/Export feature to move old files automatically to Amazon Glacier" is incorrect. Moving old data automatically to Amazon Glacier will help reduce your Amazon S3 costs, but this can be done using Amazon S3 lifecycle policies, NOT the Import/Export feature. In order to reduce your Amazon S3 costs, you should create a lifecycle policy to automatically move old (or infrequently accessed) files to less expensive storage tiers, or to automatically delete them after a specified duration.

References:

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

Question 64: **Correct**

Using Amazon EC2 falls under which of the following cloud computing models?

-
-

IaaS

(Correct)

-
-

PaaS

-

SaaS

-

IaaS & SaaS

Explanation

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. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.

For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and requires the customer to perform all of the configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for 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.

The other options are incorrect:

1- 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. A common example of a PaaS platform is the AWS Elastic Beanstalk service. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

2- 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 where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

References:

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

Question 65: **Incorrect**

Sarah has deployed an application in the Northern California (us-west-1) region. After examining the application's traffic, she notices that about 30% of the traffic is coming from Asia. What can she do to reduce latency for the users in Asia?

- Recreate the website content
- Migrate the application to a hosting provider in Asia

(Incorrect)

- Replicate the current resources across multiple Availability Zones within the same region
- Create a CDN using CloudFront, so that content is cached at Edge Locations close to and in Asia

(Correct)

Explanation

CloudFront is AWS's content delivery network (CDN) service. Amazon CloudFront employs a global network of edge locations and regional edge caches

that 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, reducing latency and improving the overall performance.

The other options are incorrect:

"Migrate the application to a hosting provider in Asia" is incorrect. AWS now can deal with most of the customers' requirements. Whatever your problem is you can find a solution.

"Recreate the website content" is incorrect. There is no relation between the website content and the traffic that comes to the web application.

"Replicate the current resources across multiple Availability Zones within the same region" is incorrect. This will only help if the replication is done in a region located in or close to Asia.

References:

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

Question 1:

Skipped

What does AWS Service Catalog provide?

- It enables customers to quickly find descriptions and use cases for AWS services
- It enables customers to explore the different catalogs of AWS services
- It simplifies organizing and governing commonly deployed IT services

(Correct)

- It allows developers to deploy infrastructure on AWS using familiar programming languages

Explanation

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows you to centrally manage commonly deployed IT services, and helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

The other options are incorrect:

"It enables customers to explore the different catalogs of AWS services" is incorrect. AWS Service Catalog doesn't contain catalogs by default. Each customer creates their own service catalog.

"It enables customers to quickly find descriptions and use cases for AWS services" is incorrect. You can find description and use cases for any service by visiting the landing page of the service (or the related documentation).

"It allows developers to deploy infrastructure on AWS using familiar programming languages" is incorrect. AWS Cloud Development Kit (AWS CDK) is the service that allows developers to model and deploy infrastructure on AWS using familiar programming languages. The AWS Cloud Development Kit (AWS CDK) is an open-source software development framework for **defining cloud infrastructure as code with modern programming languages and deploying it through AWS CloudFormation**. AWS CDK enables you to use your existing programming skills and tools, and apply those to the task of building cloud infrastructure. AWS CDK is generally available in JavaScript, TypeScript, Python, Java, and C#.

Additional Information:

What is the relationship between AWS CDK and AWS CloudFormation?

You can think of the AWS CDK as a developer-centric toolkit that leverages the full power of modern programming languages to define your AWS infrastructure as code. The CDK actually builds on AWS CloudFormation and uses it as the engine for provisioning AWS resources. Rather than using a declarative language like JSON or YAML to define your infrastructure (as is the case with CloudFormation), the CDK lets you do that in your favorite imperative programming language. This includes languages such as JavaScript, TypeScript, Java, C#, and Python. When AWS CDK applications are run, they compile down to fully formed CloudFormation JSON/YAML templates that are then submitted to the CloudFormation service for provisioning.

References:

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

Question 2:

Skipped

A company is trying to analyze the costs applied to their AWS account recently. Which of the following provides them the most granular data about their AWS costs and usage?

-
-
-

Amazon Machine Image

- ○ Amazon CloudWatch
- ○ AWS Cost Explorer
- ○ AWS Cost & Usage Report
(Correct)

Explanation

The AWS Cost & Usage Report contains the most comprehensive set of AWS cost and usage data available, including additional metadata about AWS services, pricing, and reservations (e.g., Amazon EC2 Reserved Instances (RIs)). The AWS Cost and Usage Report tracks your AWS usage and provides information about your use of AWS resources and estimated costs for that usage. You can configure this report to present the data hourly or daily. It is updated at least once a day until it is finalized at the end of the billing period. The AWS Cost and Usage Report gives you the most granular insight possible into your costs and usage, and it is the source of truth for the billing pipeline. It can be used to develop advanced custom metrics using business intelligence, data analytics, and third-party cost optimization tools.

"Amazon CloudWatch" is incorrect. Amazon CloudWatch is a monitoring service for 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 Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

"Amazon Machine Image" is incorrect. An Amazon Machine Image is used to launch Amazon EC2 instances.

"AWS Cost Explorer" is incorrect. AWS Cost Explorer helps you visualize, understand, and manage your AWS costs and usage over time. This is done via an intuitive interface that enables you to quickly create custom reports that include charts and tabular data. You can analyze your cost and usage data in aggregate (such as total costs and usage across all accounts) down to granular details (for example, m2.2xlarge costs within the Dev account tagged "project: Blackthorn"). This option is incorrect because the AWS Cost & Usage Report provides more granular data about your AWS costs and usage than what the AWS Cost Explorer provides. The AWS Cost & Usage Report is your one-stop shop for accessing the most detailed information available about your AWS costs and usage.

References:

<https://docs.aws.amazon.com/whitepapers/latest/cost-management/getting-started-with-cost-management.html>

Question 3:

Skipped

Which of the following activities supports the Operational Excellence pillar of the AWS Well-Architected Framework?

- Using AWS CloudTrail to record user activities
- Using AWS CloudFormation to manage infrastructure as code

(Correct)

- Deploying an application in multiple Availability Zones
- Using AWS Trusted Advisor to find underutilized resources

Explanation

The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework, you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to

consistently measure your architectures against best practices and identify areas for improvement.

The AWS Well-Architected Framework is based on five pillars:

- **Operational Excellence**
- **Security**
- **Reliability**
- **Performance Efficiency**
- **Cost Optimization**

The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

AWS CloudFormation can help you define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events. This will help you build a more consistent operating model and continually improve over time.

The other options are incorrect:

"Deploying an application in multiple Availability Zones" is incorrect. This statement is much more related to the **Reliability pillar**. The reliability pillar focuses on ensuring a workload performs its intended function correctly and consistently when it's expected to. A resilient workload quickly recovers from failures to meet business and customer demand. Deploying the application resources across multiple availability zones will guarantee that even if one availability zone goes down, there will still be other availability zones to run the application efficiently.

"Using AWS CloudTrail to record user activities" is incorrect. This statement is much more related to the **Security pillar**. The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data,

identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events. AWS 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.

"Using AWS Trusted Advisor to find underutilized resources" is incorrect. . This statement is much more related to the **Cost Optimization pillar**. The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding and controlling where money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending. AWS Trusted Advisor inspects your AWS environment and makes recommendations that can potentially save you money by highlighting unused resources and opportunities to reduce your bill.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/operational-excellence-pillar/wellarchitected-operational-excellence-pillar.pdf>

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

Question 4:

Skipped

TYMO Cloud Corp is looking forward to migrating their entire on-premises data center to AWS. What tool can they use to build a Business Case for moving to the AWS Cloud?

-

AWS Snowball Migration Service

-

AWS Migration Evaluator

(Correct)

-

AWS Migration Hub



AWS DMS

Explanation

A business case is the first step in your migration journey. Creating business cases on your own can be time-consuming and does not always identify the least expensive deployment and purchasing options. AWS Migration Evaluator is a migration assessment service that helps you create a directional business case for AWS cloud planning and migration.

Migration Evaluator analyzes your on-premises compute footprint, including server configuration, utilization, annual costs to operate, eligibility for bring-your-own-license, and hundreds of other parameters. Following data collection, you will quickly receive an assessment including a projected cost estimate and savings of running your on-premises workloads in the AWS Cloud. After receiving your initial assessment, your organization can work with the Migration Evaluator team to create a directional business case that best fits your organization's requirements.

The other options are incorrect:

"AWS Migration Hub" is incorrect. AWS Migration Hub provides a single location to track the progress of application migrations across multiple AWS and partner solutions.

"AWS Snowball Migration Service" is incorrect. Snowball is a petabyte-scale data transport solution that uses secure devices to transfer large amounts of data into and out of the AWS Cloud.

"AWS DMS" is incorrect. AWS Database Migration Service (AWS DMS) is used to migrate your data to and from most widely used commercial and open-source databases. AWS DMS supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle or Microsoft SQL Server to Amazon Aurora.

References:

<https://aws.amazon.com/migration-evaluator/>

Question 5:

Skipped

Which of the following AWS services can help you perform security analysis and regulatory compliance auditing? (Choose TWO)

- AWS Virtual Private Gateway
- Amazon ECS
- AWS Config

(Correct)

- AWS Batch
- Amazon Inspector

(Correct)

Explanation

With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

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 exposure, vulnerabilities, and deviations from best practices. This allows you to make security testing a more regular occurrence as part of development and IT operations.

Additional information:

One of the most important services that performs security analysis and compliance auditing is AWS CloudTrail. AWS CloudTrail simplifies your compliance audits by automatically recording and storing event logs for actions made within your AWS account. With AWS CloudTrail, you can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period of time.

The other options are incorrect:

"AWS Virtual Private Gateway" is incorrect. AWS Virtual Private Gateway allows creating hybrid cloud architecture by connecting your data center (or network) to your Amazon virtual private cloud (VPC).

"Amazon ECS" is incorrect. Amazon Elastic Container Service (Amazon ECS) is a compute service that allows you to run and scale containerized applications on AWS.

"AWS Batch" is incorrect. AWS Batch is a compute service that allows you to run hundreds of thousands of batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted.

References:

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

Question 6:

Skipped

What is the connectivity option that uses Internet Protocol Security (IPSec) to establish encrypted connectivity between an on-premises network and the AWS Cloud?

-
-

- AWS Site-to-Site VPN
(Correct)
- Internet Gateway
- AWS Direct Connect

Explanation

AWS Virtual Private Network (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 Site-to-Site VPN utilizes Internet Protocol Security (**IPSec**) to establish encrypted connectivity between your on-premises network and AWS over the Internet. With AWS Client VPN, your users can access AWS or on-premises resources from any location using a secure TLS connection.

What is IPsec?

IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.

The other options are incorrect:

"AWS Direct Connect" is incorrect. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your on-premises network or branch office site and the AWS Cloud. AWS Direct Connect is a network service that provides an alternative to using the Internet to connect customer's on-premise sites to AWS. Using AWS Direct Connect, data that would have previously been transported over the Internet can now be delivered through a private network connection between AWS and your datacenter or corporate network.

Companies of all sizes use AWS Direct Connect to establish private connectivity between AWS and datacenters, offices, or colocation environments.

"Internet Gateway" is incorrect. An internet gateway is a VPC component that allows communication between your VPC and the internet.

"AWS IQ" is incorrect. AWS IQ is a new service that enables customers to quickly find, engage, and pay AWS Certified third-party experts for on-demand project work. To get started, customers simply log into AWS IQ and describe their project needs in a few sentences. They can then chat with experts to clarify details of the project, compare proposals, review expert profiles, and select the expert who best fits their needs. After project work is delivered, the customer will be asked to approve a payment request. Once they approve the payment, the associated charges will appear on their AWS bill.

References:

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

Question 7:

Skipped

Why do many startup companies prefer AWS over traditional on-premises solutions?
(Choose TWO)

-

Using AWS, they can reduce time-to-market by focusing on business activities rather than on building and managing data centers

(Correct)

-

AWS removes the need to invest in operational expenditure

-

AWS allows them to pay later when their business succeed

-

Using AWS allows companies to replace large capital expenditure with low variable costs

(Correct)

-

AWS can build complete data centers faster than any other Cloud provider

Explanation

Instead of building and managing data centers, AWS provides startups, enterprises, and government agencies all the services they need to quickly build their business and grow faster. AWS has significantly more services, and more features within those services, than any other cloud provider – from infrastructure technologies like compute, storage, and databases – to emerging technologies, such as machine learning and artificial intelligence, data lakes and analytics, and Internet of Things. This makes it faster, easier, and more cost effective to build nearly anything they can imagine.

Capital expenditures (CapEx) are a company's major, long-term expenses. Examples of CAPEX include physical assets such as buildings, equipment, and machinery.

Instead of having to invest heavily in these Capital expenditures (e.g. physical data centers and servers) before it is known they will be used, companies can pay only when consuming AWS resources, and pay only for how much they consume. In brief, AWS replaces their investments in large capital expenditures (CAPEX) with low variable "pay-as-you-go" costs.

The other options are incorrect:

"AWS can build complete data centers faster than any other Cloud provider" is incorrect. AWS does not build out physical data centers for customers, only for itself. AWS is a Cloud Computing provider.

"AWS removes the need to invest in operational expenditure" is incorrect. Operating expenses (OpEx) are a company's day-to-day expenses. Examples of OPEX include employee salaries, rent, utilities, and property taxes. With AWS, Startups can reduce (not remove) their day to day operating expense (OpEx) costs.

"AWS allows them to pay later when their business succeed" is incorrect. AWS does not offer a "pay later" option for its customers. AWS provides three payment models: "Pay-as-you-go", "Save when you reserve" and "Pay less by using more".

References:

<https://aws.amazon.com/what-is-aws/>

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

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

Question 8:

Skipped

What are AWS shared controls?

-
-

Controls that apply to both the infrastructure layer and customer layers

(Correct)

-
-

Controls that the customer and AWS collaborate together upon to secure the infrastructure

-
-

Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services

-
-

Controls that a customer inherits from AWS

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.

The other options are incorrect:

"Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services" is incorrect because it refers to "Customer-Specific" controls.

"Controls that a customer inherits from AWS" is incorrect because it refers to "Inherited Controls".

"Controls that the customer and AWS collaborate together upon to secure the infrastructure" is incorrect. Securing the infrastructure is the responsibility of AWS, not the customer.

References:

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

Question 9:

Skipped

A company has developed a media transcoding application in AWS. The application is designed to recover quickly from hardware failures. Which one of the following types of instance would be the most cost-effective choice to use?

- Spot Instances
- (Correct)**
- On-Demand instances
- Dedicated instances
- Reserved instances

Explanation

The question stated that the application is designed to recover quickly from failures, therefore it can handle any interruption may occur with the instance. Hence, we can use the Spot instances for this application. 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 the most cost-effective choice if you are flexible about when your applications run and if your applications can be interrupted. For example, Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks.

The other options are incorrect:

"On-Demand instances" is incorrect. On-demand is not a cost-effective choice.

"Reserved instances" is incorrect. Reserved Instances provide a discount (up to 75%) compared to On-Demand instance. Even if the question stated that the company needs the instances for a year, the best answer should still be Spot Instances as they offer a greater overall cost reduction (up to 90 %) than Reserved Instances.

"Dedicated instances" is incorrect. Dedicated instances are used when you want your instances to be physically isolated at the host hardware level from instances that belong to other AWS accounts.

References:

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

Question 10:

Skipped

Why does every AWS Region contain multiple Availability Zones?

-

Multiple Availability Zones allows you to build resilient and highly available architectures

(Correct)

-

Multiple Availability Zones within a region increases the storage capacity available in that region

-

Multiple Availability Zones results in lower total cost compared to deploying in a single Availability Zone

-

Multiple Availability Zones allows for data replication and global reach

Explanation

Resilience is the ability of an architecture to continue providing the same quality of service even if some of its resources become inaccessible. Deploying your resources across multiple Availability Zones offer you the ability to operate

production applications and databases that are more resilient, highly available, and scalable than would be possible from a single data center.

The other options are incorrect:

"Multiple Availability Zones within a region increases the storage capacity available in that region" is incorrect. In AWS, you have virtually unlimited storage capacity regardless of Regions or Availability Zones in a region.

"Multiple Availability Zones results in lower total cost compared to deploying in a single Availability Zone" is incorrect. Deploying your resources across multiple availability zones has no cost benefits.

"Multiple Availability Zones allows for data replication and global reach" is incorrect. Multiple Availability Zones within a region allows for data replication but not global reach.

References:

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

Question 11:

Skipped

What is the AWS service that provides five times the performance of a standard MySQL database?

-

Amazon Aurora

(Correct)

-

Amazon Neptune

- Amazon Redshift
- Amazon DynamoDB

Explanation

Amazon Aurora is a fully-managed, MySQL and PostgreSQL-compatible relational database engine. It combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It delivers up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

The other options are incorrect:

Amazon Redshift is incorrect. Amazon Redshift is a data warehousing service.

Amazon Neptune is incorrect. Amazon Neptune is a graph database service.

Amazon DynamoDB is incorrect. Amazon DynamoDB is a NoSQL database engine.

References:

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

Question 12:

Skipped

A company needs to migrate their website from on-premises to AWS. Security is a major concern for them, so they need to host their website on hardware that is NOT shared with other AWS customers. Which of the following EC2 instance options meets this requirement?

-

Spot instances

-

Dedicated instances

(Correct)

-

On-demand instances

-

Reserved instances

Explanation

Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at the hardware level. In addition, Dedicated Instances that belong to AWS accounts that are linked to a single payer account are also physically isolated at the hardware level. However, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances.

The other options are incorrect:

"Reserved instances" and "Spot instances" and "On-demand instances" are incorrect. Reserved, Spot and On-demand instances all share hardware with other customers.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html>

Question 13:

Skipped

Which of the following are use cases for Amazon S3? (Choose TWO)

-

Cost-effective database and log storage

- A media store for the CloudFront service

(Correct)

- Hosting websites that require sustained high CPU utilization
- Processing data streams at any scale
- Hosting static websites

(Correct)

Explanation

You can host a static website on Amazon Simple Storage Service (Amazon S3). On a static website, individual webpages include static content. They might also contain client-side scripts. To host a static website, you configure an Amazon S3 bucket for website hosting, allow public read access, and then upload your website content to the bucket. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting. Amazon Web Services (AWS) also has resources for hosting dynamic websites such as Amazon EC2.

Amazon S3 is an excellent storage facility for your media assets. It is infinitely scalable, has built-in redundancy, and is available to you on a pay-as-you-go basis. For example, if you want to deliver or stream video files to your global users, all you need to do is to put your content in an S3 bucket and create a CloudFront distribution that points to the bucket. Your user's video player will use CloudFront URLs to request the video file. The request will be directed to the best edge location, based on the user's location. The Amazon Cloudfront Content Delivery Network (CDN) will serve the video from its cache, fetching it from the S3 bucket if it has not already been cached. The CDN caches content at the edge locations for consistent, low-latency, high-throughput video delivery.

The other options are incorrect:

"Cost-effective database and log storage" is incorrect. Amazon S3 can be used to store log files, images, videos (or any static content), but not databases. Databases and dynamic websites require block-level storage (such as EBS). S3 is an object-level storage, not Block-level storage. Object-level storage has limited I/O and is therefore ill-suited for use as a database store.

"Hosting websites that require sustained high CPU utilization" is incorrect. S3 can only be used to host static websites.

"Processing data streams at any scale" is incorrect. S3 is not a compute service.

References:

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

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

Question 14:

Skipped

A company wants to keep a secondary backup copy of its databases to meet regulatory requirements. Compliance policies require that the data be retrievable immediately when requested. What is the most cost-effective storage option that will meet these requirements?

-

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

(Correct)

-

Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

-

Amazon S3 Standard (S3 Standard)



Amazon S3 Glacier

Explanation

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA.

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

Although S3 One Zone-IA offers less availability than all other S3 storage classes but that is not an issue for the given scenario since it is just a secondary backup copy. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA.

The other options are incorrect:

"Amazon S3 Standard (S3 Standard)" is incorrect. Amazon S3 Standard is not a cost-effective solution for storing backups. Amazon S3 Standard is a general-purpose object storage for active and frequently accessed data. S3 Standard use cases include: cloud applications, content distribution, mobile and gaming applications, and big data analytics.

"Amazon S3 Glacier" is incorrect. Amazon S3 Glacier is more cost-effective than S3 One Zone-IA, but it does not provide immediate retrieval of data. With S3 Glacier, the minimum retrieval period is 1-5 minutes.

"Amazon S3 Standard-Infrequent Access (S3 Standard-IA)" is incorrect. Amazon S3 Standard-Infrequent Access (S3 Standard-IA) can be used to store backups, but it costs more than S3 One Zone-IA.

References:

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

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

Question 15:

Skipped

A customer is planning to move billions of images and videos to be stored on Amazon S3. The customer has approximately 60 Petabytes of data to move. Which of the following AWS Services is the best choice to transfer the data to AWS?

- Snowcone
 - S3 Transfer Acceleration
 - Snowmobile
- (Correct)**
- Snowball

Explanation

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to 100 Petabytes (PB) per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. At exabyte scale, transferring data with Snowmobile is more secure, fast and cost effective.

The other options are incorrect:

Snowcone is incorrect. Snowcone is small, edge compute and data storage product. You can use Snowcone to collect, process, and transfer data to AWS, either offline by shipping the device, or online with AWS DataSync. With 2 vCPUs, 4 GB of memory, and 8 TB of usable storage (14 TB for Snowcone SSD), all Snowcone devices can run edge computing workloads that use Amazon EC2 instances, and store data securely. You can transfer up to 8 TB with a single AWS Snowcone device and can transfer larger data sets with multiple devices, either in parallel, or sequentially. For example, you can transfer 24 TB of data with 3 Snowcone devices. This option is incorrect because Snowcone can only be used to transfer small amounts of data, not Petabytes. Remember: 1 Petabyte = 1000 Terabytes.

Snowball is incorrect. AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS using storage devices designed to be secure for physical transport. Customers can transfer up to 80 Terabytes per Snowball. In our case, the customer needs to move 60 Petabytes of data (or 60,000 Terabytes), so it is better to use the AWS Snowmobile service. Generally, to migrate large datasets of 10 Petabytes or more in a single location, you should use Snowmobile. For datasets less than 10 Petabytes or distributed in multiple locations, you should use Snowball.

Note: A single Snowball device can transport up to 80 Terabytes of data. To transfer larger amounts (for example, 3 petabytes of data), you need to use multiple Snowball devices, either in parallel or clustered together.

S3 Transfer Acceleration is incorrect. Amazon S3 Transfer Acceleration uses the internet to transfer data into and out of AWS. Even with high-speed internet connections, it can take years to transfer 60 Petabytes of data. The Snowmobile is designed to transfer data at a rate of up to 1 Tb/s, which means you could fill a 100PB Snowmobile in less than 10 days.

What is Amazon S3 Transfer Acceleration?

Amazon S3 Transfer Acceleration enables fast transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path. If you are uploading to a centralized bucket from geographically dispersed locations, or if you regularly transfer GBs or TBs of data across continents, you may save hours or days of data transfer time with S3 Transfer Acceleration.

References:

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

Question 16:**Skipped**

A company needs to track resource changes using the API call history. Which AWS service can help the company achieve this goal?



AWS Config



AWS CloudTrail

(Correct)

AWS CloudFormation



Amazon CloudWatch

Explanation

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. With CloudTrail, you can get a history of AWS API calls for your account, including API calls made using the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

The other options are incorrect:***"AWS Config" is incorrect.***

Both AWS Config and AWS CloudTrail can be used to track resource changes, and it is very important to distinguish between them. AWS Config is used to monitor and audit changes in AWS resources and allow you to automate the evaluation of recorded configurations of a specific resource against desired configurations. AWS CloudTrail records user API activity on your account and allows you to access information about this activity. You get full details about API actions, such as identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service.

AWS Config records point-in-time configuration details for your AWS resources as Configuration Items (CIs). You can use a CI to answer "What did my AWS resource look like?" at a point in time. You can use AWS CloudTrail to answer "Who made an API call to modify this resource?" For example, you can use the AWS Management Console for AWS Config to detect security group "Production-DB" was incorrectly configured in the past. Using the integrated AWS CloudTrail information, you can pinpoint which user misconfigured "Production-DB" security group. In brief, AWS Config provides information about the changes made to a resource, and AWS CloudTrail provides information about who made those changes.

"AWS CloudFormation" is incorrect. AWS CloudFormation is a service that allows you to use 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 CloudWatch" is incorrect. Amazon CloudWatch is used to monitor and collect custom and granular metrics about your AWS resources.

References:

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

Question 17:

Skipped

Which of the following is NOT a characteristic of Amazon Elastic Compute Cloud (Amazon EC2)?

-

Amazon EC2 offers scalable computing

- Amazon EC2 eliminates the need to invest in hardware upfront
- Amazon EC2 is considered a Serverless Web Service

(Correct)

- Amazon EC2 can launch as many or as few virtual servers as needed

Explanation

"**Amazon EC2 is considered a Serverless Web Service**" is not a characteristic of Amazon EC2 and thus is the correct choice. Serverless allows customers to shift more operational responsibilities to AWS. Serverless allows customers to build and run applications and services without thinking about servers. Serverless eliminates infrastructure management tasks such as server or cluster provisioning, patching, operating system maintenance, and capacity provisioning.

Amazon EC2 is not a serverless service. EC2 instances are virtual servers in the cloud. Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware upfront, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html>

Question 18:

Skipped

Which of the following allows you to create new RDS instances? (Choose TWO)

- AWS CloudFormation

(Correct)

- AWS Quick Starts
- AWS DMS
- AWS CodeDeploy
- AWS Management Console
(Correct)

Explanation

The AWS Management Console lets you create new RDS instances through a web-based user interface.

You can also use AWS CloudFormation to create new RDS instances using the CloudFormation template language.

The other options are incorrect:

"AWS DMS" is incorrect. AWS DMS is used to migrate databases to AWS.

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

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

References:

<https://docs.aws.amazon.com/awsconsolehelpdocs/index.html>

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

Question 19:

Skipped

How do ELBs improve the reliability of your application?

- By distributing traffic across multiple S3 buckets
- By replicating data to multiple availability zones
- By creating database Read Replicas
- By ensuring that only healthy targets receive traffic

(Correct)

Explanation

The reliability term encompasses the ability of a system to recover from infrastructure or service disruptions, and dynamically acquire computing resources to meet demand. ELBs continuously perform health checks on the registered targets (such as Amazon EC2 instances) and only routes traffic to the healthy ones. This increases the fault tolerance of your application and makes it more reliable.

The other options are incorrect:

"By replicating data to multiple availability zones" is incorrect. ELBs are not responsible for replicating data.

"By creating database Read Replicas" is incorrect. Read Replicas are special types of database instances that are part of Amazon RDS NOT ELB. The purpose of Read Replicas on Amazon RDS is to enhance database performance and increase database availability.

"By distributing traffic across multiple S3 buckets" is incorrect. There is no need to create multiple S3 buckets and distribute traffic between them; One S3 bucket can handle any amount of traffic without any intervention. Amazon S3 was designed from the ground up to handle traffic for any Internet application. Amazon S3's massive scale allows to spread load evenly, so that no individual application is affected by traffic spikes.

References:

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

Question 20:

Skipped

What is the benefit of using an API to access AWS Services?

-
-

It reduces the time needed to provision AWS resources

-
-

It allows for programmatic management of AWS resources

(Correct)

-
-

It improves the performance of AWS resources

-
-

It reduces the number of developers necessary

Explanation

The AWS Application Programming Interface (API) allows customers to work with various AWS services programmatically.

The other options are incorrect:

"It improves the performance of AWS resources" is incorrect. There is no difference in performance when you provision resources using the console or using the AWS API. In fact, if you access AWS through the AWS Management Console or through the command line tools, you are actually using tools that make calls to the AWS API.

"It reduces the time needed to provision AWS resources" is incorrect. Since AWS Console and AWS CLI both provision resources by making AWS API calls, then there will be no difference in the time needed to provision these resources using either of them.

"It reduces the number of developers necessary" is incorrect. Depending on the use case, using the AWS API may actually require more developers to manage AWS resources programmatically.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/APIReference/making-api-requests.html>

Question 21:

Skipped

Which of the following can be used to protect data at rest on Amazon S3? (Choose TWO)

- Deduplication
- Versioning

(Correct)

-

Permissions

(Correct)

-

Decryption

-

Conversion

Explanation

Amazon S3 provides a number of security features for the protection of data at rest, which you can use or not depending on your threat profile:

1- Permissions: Use bucket-level or object-level permissions alongside IAM policies to protect resources from unauthorized access and to prevent information disclosure, data integrity compromise or deletion.

2- Versioning: Amazon S3 supports object versions. Versioning is disabled by default. Enable versioning to store a new version for every modified or deleted object from which you can restore compromised objects if necessary.

3- Replication: Although Amazon S3 stores your data across multiple geographically diverse Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-region replication (CRR) allows you to replicate data between distant AWS Regions to help satisfy these requirements. CRR enables automatic, asynchronous copying of objects across buckets in different AWS Regions.

4- Encryption – server side: Amazon S3 supports server-side encryption of user data. Server-side encryption is transparent to the end user. AWS generates a unique encryption key for each object, and then encrypts the object using AES-256.

5- Encryption – client side: With client-side encryption you create and manage your own encryption keys. Keys you create are not exported to AWS in clear text. Your applications encrypt data before submitting it to Amazon S3, and decrypt data after receiving it from Amazon S3. Data is stored in an encrypted form, with keys and algorithms only known to you.

Additional information: (IMPORTANT)

AWS also provides a fully managed security service called AWS Macie to help protect your sensitive data in Amazon S3. Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in Amazon S3. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks. Today, Amazon Macie is available to protect data stored in Amazon S3, with support for additional AWS data stores coming later this year.

The other options are incorrect:

"Deduplication" is incorrect. Deduplication is the process of removing duplicate data, and will do nothing to prevent data loss of data at rest.

"Conversion" is incorrect. Conversion is the process of transforming data from one format to another.

"Decryption" is incorrect. Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>

Question 22:

Skipped

What is the framework created by AWS Professional Services that helps organizations design a road map to successful cloud adoption?



Amazon EFS



AWS WAF



AWS CAF

(Correct)



AWS Secrets Manager

Explanation

AWS Professional Services created the AWS Cloud Adoption Framework (AWS CAF) to help organizations design and travel an accelerated path to successful cloud adoption. The guidance and best practices provided by the framework help you build a comprehensive approach to cloud computing across your organization, and throughout your IT lifecycle. Using the AWS CAF helps you realize measurable business benefits from cloud adoption faster and with less risk.

The other options are incorrect:

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

"Amaozn EFS" is incorrect. Amazon Elastic File System (Amazon EFS) Amazon EFS is a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud. Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance.

"AWS WAF" is incorrect. AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define.

References:

<https://aws.amazon.com/professional-services/CAF/>

Question 23:

Skipped

Which statement best describes the concept of an AWS region?

- An AWS Region is a geographical location with a collection of Availability Zones
(Correct)
- An AWS Region represents the country where the AWS infrastructure exist
- An AWS Region is a geographical location with a collection of Edge locations
- An AWS Region is a virtual network dedicated only to a single AWS customer

Explanation

An AWS Region is a physical location in the world. Each region has multiple, isolated locations known as Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity. These Availability Zones offer you the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible to operate out of a single data center. Also, each AWS Region is designed to be completely isolated from the other AWS Regions. This achieves the greatest possible fault tolerance and stability.

References:

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

Question 24:

Skipped

What is the AWS tool that can help a company visualize their AWS spending in the last few months?



AWS Budgets



AWS Pricing Calculator



AWS Cost Explorer

(Correct)



AWS Consolidated Billing

Explanation

The AWS Billing and Cost Management console includes the Cost Explorer tool for viewing AWS cost data as a graph. The user can filter the graphs using the resource tags. If the company is using Consolidated Billing, it generates a report based on the linked accounts which can help to identify areas that require further inquiry. Using the Cost Explorer, the company can view trends and use them to understand their spending and to predict future costs.

The other options are incorrect:

"AWS Pricing Calculator" is incorrect. The AWS Pricing Calculator helps customers and prospects **estimate** their monthly AWS bill more efficiently.

AWS Pricing Calculator does not provide any information about your actual AWS spend or usage. You can access and use [AWS Pricing Calculator](#) even if you do not have an AWS account. AWS Pricing Calculator only provides an estimate of your

monthly AWS bill based on your expected usage (e.g., how much storage you expect to use).

"AWS Consolidated Billing" is incorrect. Consolidated billing is a feature in AWS Organizations that you can use to consolidate billing and payment for multiple AWS accounts.

"AWS Budgets" is incorrect. AWS Budgets allows you to set custom budgets that alert you when you exceed your budgeted thresholds.

References:

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

Question 25:

Skipped

AWS recommends some practices to help organizations avoid unexpected charges on their bill. Which of the following is NOT one of these practices?

- Deleting unused Elastic Load Balancers
- Deleting unused AutoScaling launch configuration

(Correct)

- Deleting unused EBS volumes after terminating an EC2 instance
- Releasing unused Elastic IPs after terminating an EC2 instance

Explanation

"Deleting unused AutoScaling launch configuration" will not help, and thus is the correct choice. The AutoScaling launch configuration does not incur any charges. Thus, it will not make any difference whether it is deleted or not.

AWS will charge the user once the AWS resource is allocated (even if it is not used). Thus, it is advised that once the user's work is completed they should:

- 1- Delete all Elastic Load Balancers.
- 2- Terminate all unused EC2 instances.
- 3- Delete the attached EBS volumes that they don't need.
- 4- Release any unused Elastic IPs.

Additional information:

Some services automatically restart resources after terminating them without notifying you, and as a result, you get unexpected charges on your bill.

Examples of these services:

1- Elastic Beanstalk:

Elastic Beanstalk is designed to ensure that all the resources that you need are running, which means that it automatically relaunches any service that you stop. If you need to permanently delete those resources you must terminate your Elastic Beanstalk environment before you terminate resources that Elastic Beanstalk has created.

2- AWS OpsWorks:

If you use the AWS OpsWorks environment to create AWS resources, you must use AWS OpsWorks to terminate those resources or AWS OpsWorks will restart them. For example, if you use AWS OpsWorks to create an Amazon EC2 instance, but then stop it by using the Amazon EC2 console, the AWS OpsWorks auto-healing feature categorizes the instance as failed and restarts it.

References:

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

Question 26:

Skipped

Which AWS Service is used to manage user permissions?

- Security Groups
- AWS IAM
(Correct)
- AWS Support
- Amazon ECS

Explanation

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

The other options are incorrect:

"Amazon ECS" is incorrect. Amazon ECS is used to run containerized applications on AWS.

"Security Groups" is incorrect. Security Groups is not an AWS service. Security Groups is a networking feature that allows customers to control instance traffic.

"AWS Support" is incorrect. AWS Support is not an AWS service. The AWS Support team cannot modify user permissions on customer's behalf. It is the responsibility of the customer to manage all access permissions.

References:

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

Question 27:

Skipped

How can AWS customers track and avoid over-spending on underutilized reserved instances?

-
- Customers can use Amazon Neptune to track and analyze their usage patterns, detect underutilized reserved instances, and then sell them on the Amazon EC2 Reserved Instance Marketplace
-
- Customers can use Amazon CloudTrail to automatically check for unused reservations and get recommendations to reduce their bill
-
- Customers can add all AWS accounts to an AWS Organization, enable Consolidated Billing, and turn off Reserved Instance sharing
-
- Customers can use the AWS Budgets service to track the reserved instances usage and set up alert notifications when their utilization drops below the threshold that they define

(Correct)

Explanation

There are three main types of Budgets that Customers can create using the AWS Budgets service:

1- Cost Budgets:

AWS Cost Budgets gives customers the ability to set custom budgets that alert them when their costs exceed (or are forecasted to exceed) their budgeted amount.

2- Usage Budgets:

AWS Usage Budgets can alert customers when their usage exceeds (or is forecasted to exceed) the thresholds they define.

3- Reservation Budgets:

Customers can use the Reservation Budgets to set reservation utilization or coverage targets and receive alerts when their utilization drops below the threshold they define. This will help AWS customers track the utilization of their reserved instances and avoid over-spending on unused reservations.

The other options are incorrect:

"Customers can use Amazon CloudTrail to automatically check for unused reservations and get recommendations to reduce their bill" is incorrect. AWS Trusted Advisor is the service that automatically checks for unused reservations and provides recommendations to reduce costs.

AWS 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.

"Customers can use Amazon Neptune to track and analyze their usage patterns, detect underutilized reserved instances, and then sell them on the Amazon EC2 Reserved Instance Marketplace" is incorrect. Amazon Neptune is a graph database service, not a monitoring service. Amazon Neptune can not be used to track or analyze AWS customers' usage.

You can use Amazon Neptune to build and run applications that work with highly connected datasets, such as social networking, recommendation engines, and knowledge graphs.

"Customers can add all AWS accounts to an AWS Organization, enable Consolidated Billing, and turn off Reserved Instance sharing" is incorrect. 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. But if you turn off Reserved Instance sharing, none of the accounts will receive the hourly cost benefit of the Reserved Instances.

Additional information:

The management account (payer account) of an organization can turn off Reserved Instance (RI) discount sharing for any accounts in that organization, including the payer account. This means that RIs discounts aren't shared between any accounts that have sharing turned off. To share an RI discount with an account, both accounts must have sharing turned on.

References:

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

Question 28:

Skipped

Which AWS service provides cost-optimization recommendations?



AWS Trusted Advisor

(Correct)



AWS X-Ray



AWS Pricing Calculator



Amazon QuickSight

Explanation

AWS Trusted Advisor is an application that draws upon best practices learned from AWS' aggregated operational history of serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and makes recommendations that can potentially save you money by highlighting unused resources and opportunities to reduce your bill. AWS Trusted Advisor also provide recommendations to improve system performance, and close security gaps.

The other options are incorrect:

"Amazon QuickSight" is incorrect. Amazon QuickSight is a serverless, machine learning-powered business intelligence (BI) service built for the cloud. QuickSight lets you easily **create and publish interactive BI dashboards** that include Machine Learning-powered insights. QuickSight dashboards can be accessed from any device, and seamlessly embedded into your applications, portals, and websites.

Unlike traditional BI or data discovery solutions, getting started with Amazon QuickSight is simple and fast. When you log in, Amazon QuickSight seamlessly discovers your data sources in AWS services such as Amazon Redshift, Amazon RDS, Amazon Athena, and Amazon Simple Storage Service (Amazon S3). You can connect to any of the data sources discovered by Amazon QuickSight and get insights from this data in minutes. Amazon QuickSight supports rich data discovery and business analytics capabilities to help customers derive valuable insights from their data without worrying about provisioning or managing infrastructure.

"AWS X-Ray" is incorrect. AWS X-Ray can be used to analyze and debug your production applications and helps you understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.

"AWS Pricing Calculator" is incorrect. The AWS Pricing Calculator does not provide cost-optimization recommendations. It helps you estimate the cost for your AWS monthly bill based on your expected usage.

References:

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

Question 29:

Skipped

What is the most cost-effective purchasing option for running a set of EC2 instances that must always be available for a period of two months?

- Reserved Instances - No Upfront
-

On-Demand Instances

(Correct)

-
- Spot Instances
-
- Reserved Instances - All Upfront

Explanation

The most cost-effective option for this scenario is to use On-Demand Instances.

The other options are incorrect:

"Spot Instances" is incorrect. AWS Spot instances can be interrupted at any time by AWS. You should only choose Spot instances if the question clearly stated that the application can handle interruptions or if continuous processing is not required. Usually Spot instances are used for batch processing jobs or for non-production applications, such as development and test servers, where occasional downtime is acceptable.

"Reserved Instances - All Upfront" and "Reserved Instances - No Upfront" are incorrect. Since the duration is just for two months, we should use On-demand instances. Reserved instances require a purchase term of at least one year.

References:

<https://aws.amazon.com/ec2/pricing/on-demand/>

Question 30:

Skipped

What is the minimum level of AWS support that provides 24x7 access to technical support engineers via phone and chat?

-

Enterprise Support

-

Developer Support

-

Basic Support

-

Business Support

(Correct)

Explanation

Each of the Business and Enterprise support plans provide 24x7 access to technical support engineers via phone, email, and chat. The Business Support Plan is less expensive than the Enterprise Support Plan. Therefore, the correct answer is Business.

The other options are incorrect:

"Basic Support" is incorrect. The technical support is not available for the Basic support plan.

"Developer Support" is incorrect. Developer support plan provides business hours access to technical support associates via email only.

References:

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

Question 31:

Skipped

A company is planning to migrate an application from Amazon EC2 to AWS Lambda to use a serverless architecture. Which of the following will be the responsibility of AWS after migration? (Choose TWO)

- Capacity management
(Correct)
- Operating system maintenance
(Correct)
- Access control
- Data management
- Application management

Explanation

For AWS Lambda, AWS manages the underlying infrastructure and foundation services, the operating system, the runtime environment, and the application platform. AWS Lambda performs all the operational and administrative activities on the customer's behalf, including operating system maintenance, provisioning and scaling compute capacity to maintain consistent performance, monitoring fleet health, applying security patches to the underlying compute resources, encrypting code, deploying code, and running a web service front end.

AWS Lambda enables customers to run their applications without provisioning or managing servers. AWS customers are only responsible for building and managing their applications, managing their data, and controlling access to the Lambda service and within their Lambda Functions.

The other options are incorrect:

"Data management" is incorrect. Data management is a customer responsibility.

"Application management" is incorrect. Application management is a customer responsibility.

"Access control" is incorrect. Access control is a customer responsibility.

References:

<https://docs.aws.amazon.com/whitepapers/latest/security-overview-aws-lambda/the-shared-responsibility-model.html>

Question 32:

Skipped

Which of the following are factors in determining the appropriate database technology to use for a specific workload? (Choose TWO)

-

The nature of the queries

(Correct)

-

The number of reads and writes per second

(Correct)

-

Data sovereignty

-

Software bugs

-

Availability Zones

Explanation

The following questions can help you take decisions on which solutions to include in your architecture:

- Is this a read-heavy, write-heavy, or balanced workload? How many reads and writes per second are you going to need? How will those values change if the number of users increases?
- How much data will you need to store and for how long? How quickly do you foresee this will grow? Is there an upper limit in the foreseeable future? What is the size of each object (average, min, max)? How are these objects going to be accessed?
- What are the requirements in terms of durability of data? Is this data store going to be your "source of truth"?
- What are your latency requirements? How many concurrent users do you need to support?
- What is your data model and how are you going to query the data? Are your queries relational in nature (e.g., JOINs between multiple tables)? Could you denormalize your schema to create flatter data structures that are easier to scale?
- What kind of functionality do you require? Do you need strong integrity controls or are you looking for more flexibility (e.g., schema-less data stores)? Do you require sophisticated reporting or search capabilities? Are your developers more familiar with relational databases than NoSQL?

The other options are incorrect:

"Data sovereignty" is incorrect. Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Data sovereignty is a factor you should consider when choosing your AWS region NOT the database.

"Software bugs" is incorrect. A software bug is an error, flaw, failure, or fault in a system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways. Most bugs are due to human errors made in source code or software design, so if software has bugs, you have to search for a fix. Database

technologies cannot help you with application bugs, as they provide services related only to databases.

"Availability Zones" is incorrect. Availability zones in a region are all relatively the same. There is no reason to prefer any Availability Zone in which to run a database.

References:

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

Question 33:

Skipped

A company has discovered that multiple S3 buckets were deleted, but it is unclear who deleted the buckets. Which of the following can the company use to determine the identity that deleted the buckets?

- CloudWatch Logs
- CloudTrail logs
- SQS logs
- SNS logs

(Correct)

Explanation

AWS CloudTrail is a web service that records all AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller (who deleted the buckets in our case), the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. With CloudTrail, you can get a history of AWS API calls for your account, including API calls made using the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS

CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

The other options are incorrect:

"SNS logs" is incorrect. SNS is not for logging API calls, it is a fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

"CloudWatch Logs" is incorrect. Amazon CloudWatch Logs are not used to record user interactions with AWS. You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources.

"SQS logs" is incorrect. SQS is not for logging API calls, it is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

Question 34:

Skipped

A developer needs to set up an SSL security certificate for a client's eCommerce website in order to use the HTTPS protocol. Which of the following AWS services can be used to deploy the required SSL server certificates? (Choose TWO)

-

AWS Identity & Access Management

(Correct)

- AWS ACM
(Correct)
- AWS Data Pipeline
- Amazon Route 53
- AWS Directory Service

Explanation

To enable HTTPS connections to your website or application in AWS, you need an SSL/TLS server certificate. You can use a server certificate provided by AWS Certificate Manager (ACM) or one that you obtained from an external provider. You can use ACM or IAM to store and deploy server certificates. Use IAM as a certificate manager only when you must support HTTPS connections in a region that is not supported by ACM. IAM supports deploying server certificates in all regions, but you must obtain your certificate from an external provider for use with AWS. Amazon Route 53 is used to register domain names or use your own domain name to route your end users to Internet applications. Route 53 is not responsible for creating SSL certifications.

The other options are incorrect:

"AWS Directory Service" is incorrect. AWS Directory Service is a managed Microsoft Active Directory in the AWS Cloud. Customers can use it to manage users and groups, provide single sign-on (SSO) to applications and services, as well as create and apply group policies.

Note: What is Single sign-on (SSO)? Single sign-on (SSO) enables a company's employees to sign in to AWS using their existing corporate Microsoft Active Directory credentials.

"Amazon Route 53" is incorrect. Amazon Route 53 can be used for registering domain names, routing end users to Internet applications, configuring DNS health checks to route traffic to healthy endpoints, managing traffic globally through a variety of routing types etc.

"AWS Data Pipeline" is incorrect. AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources. AWS Data Pipeline integrates with on-premise and cloud-based storage systems to allow developers to use their data when they need it, where they want it, and in the required format.

References:

<https://aws.amazon.com/certificate-manager/>

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_server-certs.html

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

Question 35:

Skipped

What is the AWS IAM feature that provides an additional layer of security on top of user-name and password authentication?

-
- MFA

(Correct)

-
- SDK
-
- Access Keys
-
- Key Pair

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:

"Access Keys" is incorrect. Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

"Key Pair" is incorrect. The AWS Key pair cryptography enables you to securely access your Amazon EC2 instances using a private key instead of a password.

"SDK" is incorrect. AWS SDKs are used to simplify using AWS services in your applications with an API tailored to your programming language or platform. AWS SDKs in AWS include Java SDK, .NET SDK, Node.js SDK and many others.

References:

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

Question 36:

Skipped

What are the benefits of using the Amazon Relational Database Service? (Choose TWO)

-

Scales automatically to larger or smaller instance types

-

Complete control over the underlying host

-

Resizable compute capacity

(Correct)

-

Lower administrative burden

(Correct)

-

Supports the document and key-value data structure

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 and resizable Compute (and\or Storage) 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.

The other options are incorrect:

"Complete control over the underlying host" is incorrect. The user doesn't have access to the underlying host. For managed services like this, AWS is responsible for performing all the operations needed to keep the service running.

"Supports the document and key-value data structure" is incorrect. RDS doesn't support document and key-value data structures. The AWS service that support them is DynamoDB.

"Scales automatically to larger or smaller instance types" is incorrect. Amazon RDS provides you with six widely-used database engines to choose from,

including **Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server**. The only RDS database that can scale instances automatically is Amazon Aurora.

Additional information:

For RDS databases other than Aurora, RDS only supports storage auto-scaling, NOT instance auto-scaling. If you want to scale Amazon RDS instances (other than Aurora), you have two options:

- 1- Manual horizontal scaling (by adding read replicas)
- 2- Manual vertical scaling (by upgrading/downgrading an existing instance).

References:

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

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

<https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/>

Question 37:

Skipped

Which AWS Service provides the current status of all AWS Services in all AWS Regions?

-
- Amazon CloudWatch
-
- AWS Personal Health Dashboard
-
- AWS Service Health Dashboard

(Correct)

-

AWS Management Console

Explanation

AWS uses the Service Health Dashboard to publish most up-to-the-minute information on AWS service availability. You can get information about the current status and availability of any AWS service any time using the AWS Service Health Dashboard that is available at this link: <https://status.aws.amazon.com/>

The other options are incorrect.

"AWS Personal Health Dashboard" is incorrect. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view of the status of the AWS services that power your applications (i.e. not all services), 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 the root cause.

"Amazon CloudWatch" is incorrect. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

"AWS Management Console" is incorrect. AWS Management Console allows you to access and manage Amazon Web Services through a simple and intuitive web-based user interface.

References:

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

Question 38:

Skipped

What is the AWS Compute service that executes code only when triggered by events?



AWS Transit Gateway



AWS Lambda

(Correct)



Amazon CloudWatch



Amazon EC2

Explanation

AWS Lambda is a serverless compute service that runs code in response to events. For example, you can create a Lambda function that creates thumbnail images when users upload images to Amazon S3. The Lambda event, in this case, will be the user's uploads. Once a user uploads an image to Amazon S3, AWS Lambda will automatically run the application and creates a thumbnail for that image.

The other options are incorrect:

AWS Transit Gateway is incorrect. AWS Transit Gateway is a network transit hub that customers can use to interconnect their virtual private clouds (VPCs) and their on-premises networks. AWS transit gateway simplifies how customers interconnect all of their VPCs, across thousands of AWS accounts and into their on-premises networks.

"Amazon EC2" is incorrect. After provisioning an EC2 instance, it continues to run all the time until being stopped or terminated. But with Lambda, the application code will run only when triggered.

"Amazon CloudWatch" is incorrect. Amazon CloudWatch is a monitoring service, not a compute service.

References:

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

Question 39:

Skipped

What is the AWS' recommendation regarding access keys?

- Only share them with trusted people
- Rotate them regularly

(Correct)

- Delete all access keys and use passwords instead
- Save them within your application code

Explanation

AWS recommends that you change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources.

The other options are incorrect:

"Save them within your application code" is incorrect. It is not secure to save any type of credentials within your application code.

"Only share them with trusted people" is incorrect. AWS recommends that you do not ever share your credentials with anyone.

"Delete all access keys and use passwords instead" is incorrect. Usernames and passwords are used to sign in to the AWS management console. They cannot be used to sign programmatic requests to the AWS CLI or AWS API like access keys.

References:

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

Question 40:

Skipped

Which AWS Service can be used to register a new domain name?



Amazon Route 53

(Correct)



Amazon Personalize



AWS Config



AWS KMS

Explanation

Amazon Route 53 can be used for:

- Registering domain names
- DNS routing
- Configuring health checks to route traffic only to healthy endpoints

- Managing global application traffic (cross-regions) through a variety of routing types.

Amazon Route53 allows for registration of new domain names in AWS. Amazon Route 53 is a global service that provides a highly available and scalable Domain Name System (DNS) in the Cloud. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other.

Amazon Route 53 also offers health checks to monitor the health and performance of your application, as well as your web servers and other resources. Route 53 can be configured to route traffic only to the healthy endpoints to achieve greater levels of fault tolerance in your applications.

Amazon Route 53 provides many routing types to help AWS Customers improve their application's performance for a global audience. For example, Amazon Route 53 latency-based policy routes user requests to the closest AWS Region, which reduces latency and improves application performance.

Amazon 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:

"AWS KMS" is incorrect. AWS KMS is a managed service that enables you to easily encrypt your data. 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.

"Amazon Personalize" is incorrect. Amazon Personalize is a fully managed machine learning service that can be used to deliver highly customized recommendations to customers across industries such as retail, media and entertainment. Amazon Personalize enables developers to build applications with the same machine learning (ML) technology used by Amazon.com for real-time personalized recommendations. Amazon Personalize can be used to personalize the end-user experience over any digital channel. Examples include product

recommendations for e-commerce, news articles and content recommendation for publishing, media and social networks, hotel recommendations for travel websites, and credit card recommendations for banks.

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

References:

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

Question 41:

Skipped

Why would an organization decide to use AWS over an on-premises data center?
(Choose TWO)

- Free commercial software licenses
- Free technical support
- On-site visits for auditing
- Elastic resources

(Correct)

- Cost Savings

(Correct)

Explanation

AWS continues to lower the cost of cloud computing for its customers. AWS recently lowered prices again for compute, storage, caching, and database services for all customers, making everything from web apps to big data on AWS even more cost-effective and widening the TCO gap with traditional infrastructure.

Elasticity is a system's ability to monitor user demand and automatically increase and decrease deployed resources accordingly. Elasticity is one of the most important advantages of AWS. The purpose of elasticity is to match the resources allocated with actual amount of resources needed at any given point in time. This ensures that you are only paying for the resources you actually need.

The other options are incorrect:

"Free technical support" is incorrect. Technical support is not free in AWS. Technical Support requires subscription to an AWS Support Plan.

"On-site visits for auditing" is incorrect. AWS does not allow on-site visits to its datacenters under any circumstances.

"Free commercial software licenses" is incorrect. Neither AWS nor on-premises datacenters provide free commercial software licenses. However, AWS allows you to pay for these licenses as-you-go. For example, using license included windows instances allows you access to fully compliant Microsoft software licenses bundled with Amazon EC2 or Amazon RDS instances and pay for them as you go with no upfront costs or long-term investments.

References:

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

Question 42:

Skipped

For managed services like Amazon DynamoDB, which of the below is AWS responsible for? (Choose TWO)

- Operating system maintenance
(Correct)
- Protecting credentials
- Patching the database software
(Correct)
- Creating access policies
- Logging access activity

Explanation

AWS has increased responsibilities for its managed services. Examples of managed services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, and Amazon WorkSpaces. These services provide the scalability and flexibility of cloud-based resources with less operational overhead because AWS handle basic security tasks like guest operating system (OS) and database patching, installing antivirus software, backup, and disaster recovery. For most managed services, you only configure logical access controls and protect account credentials, while maintaining control and responsibility of any personal data.

Note:

If you are using Amazon EC2 instead of the AWS managed services to run your databases and applications, you will be responsible for performing all of the necessary security configuration and management tasks.

The other options are incorrect:

"Creating access policies" is incorrect. The customer is responsible for creating the required access policies for all users using the Identity and Access Management service.

"Protecting credentials" is incorrect. The customer (or anyone in their team) is responsible for protecting their credentials.

"Logging access activity" is incorrect. Logging user access activities is the responsibility of the customer, whether they are using a managed service or any other services. The AWS customer can use AWS CloudTrail to record and monitor all API calls made in their AWS account.

References:

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

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

Question 43:

Skipped

Which of the following statements describes the AWS Cloud's agility?

- AWS allows you to host your applications in multiple regions around the world
- AWS allows you to pay upfront to reduce costs
- AWS provides customizable hardware at the lowest possible cost
- AWS allows you to provision resources in minutes

(Correct)

Explanation

In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks (or months in some cases) 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.

In other words, instead of waiting weeks or months for hardware, you can instantly deploy new applications. Also, whether you need one virtual server or thousands, whether you need them for a few hours or 24/7, you still only pay for what you use.

The other options are incorrect:

"AWS provides customizable hardware at the lowest possible cost" is incorrect. AWS doesn't provide customizable hardware. AWS offers cloud computing services.

"AWS allows you to pay upfront to reduce costs" is incorrect. This statement is much more related to AWS reservations, not agility.

"AWS allows you to host your applications in multiple regions around the world" is incorrect. It is true that AWS provides global infrastructure, but this statement doesn't describe AWS' agility.

References:

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

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

Question 44:

Skipped

Which of the following is used to control network traffic in AWS? (Choose TWO)

-

Network Access Control Lists (NACLs)

(Correct)

-

Security Groups

(Correct)

-

Key Pairs

-

IAM Policies

-

Access Keys

Explanation

You can control network traffic in AWS by configuring security groups, network access control lists, and route tables.

1- Security groups: Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

2- Network access control lists (ACLs): Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.

3- Route Tables: A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.

Note:

Controlling network traffic using any of the above methods is the responsibility of the customer.

The other options are incorrect:

"Access keys" is incorrect. Access keys are long-term credentials for an IAM user or the AWS account root user. Access keys allows you to interact with AWS services programmatically using the AWS CLI or the AWS SDK.

"IAM Policies" is incorrect. By default, IAM users don't have permission to create or modify resources in AWS. IAM policies are used to grant IAM users permission to use the specific resources and API actions they'll need.

"Key Pairs" is incorrect. Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. Public-key cryptography uses a public key to encrypt a piece of data, and then the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair. Public-key cryptography enables you to securely access your instances using a private key instead of a password.

References:

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

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

Question 45:

Skipped

When running a workload in AWS, the customer is NOT responsible for: (Select TWO)

- Auditing and regulatory compliance
- Running penetration tests
-

Infrastructure security

(Correct)

- Reserving capacity
- Data center operations

(Correct)

Explanation

AWS is responsible for the infrastructure security and all data center operations such as racking, stacking, and powering servers, so customers can focus on revenue generating activities rather than on IT infrastructure.

The other options are incorrect:

"Reserving capacity" is incorrect. Amazon does not perform reservations for a customer; capacity reservation is a customer action.

"Running penetration tests" 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 the responsibility of the customer.

"Auditing and regulatory compliance" is incorrect. There are many services on AWS to use for auditing and compliance such as AWS CloudTrail, AWS Config and Amazon Inspector. However, these services must be configured by the customer, not by AWS.

References:

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

Question 46:

Skipped

Which of the following is a benefit of running an application in multiple Availability Zones?

-
-

Increases available compute capacity

-
-

Increases the availability of your application

(Correct)

-
-

Reduces application response time between servers and global users

-
-

Allows you to exceed AWS service limits

Explanation

Placing instances that run your application in multiple Availability Zones improves the fault tolerance of your application. If one Availability Zone experiences an outage, traffic is routed to another Availability Zone, and this will increase the availability of your application.

The other options are incorrect:

"Increases available compute capacity" is incorrect. You can provision virtually unlimited compute capacity regardless of the number of Availability Zones.

"Reduces application response time between servers and global users" is incorrect. The question didn't mention whether these Availability Zones exists within a single region or multiple regions. Application response time for global users can only be improved if you deploy to multiple regions around the world.

"Allows you to exceed AWS service limits" is incorrect. AWS service limits are region-specific NOT AZ-specific.

References:

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

Question 47:

Skipped

App development companies move their business to AWS to reduce time-to-market and improve customer satisfaction, what are the AWS automation tools that help them deploy their applications faster? (Choose TWO)

- AWS CloudFormation

(Correct)

- AWS Migration Hub
- AWS Elastic Beanstalk

(Correct)

- AWS IAM
- Amazon Macie

Explanation

AWS Elastic Beanstalk makes it easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

AWS CloudFormation automates and simplifies the task of repeatedly and predictably creating groups of related resources that power your applications. Creating and interconnecting all resources your application needs to run is now as simple as creating a single EC2 or RDS instance.

The other options are incorrect.

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

"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 groups, and use permissions to allow and deny their access to AWS resources.

"AWS Migration Hub" is incorrect. AWS Migration Hub is used to track the progress of application migrations to AWS.

References:

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

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

Question 48:

Skipped

Data security is one of the top priorities of AWS. How does AWS deal with old storage devices that have reached the end of their useful life?

-
-

AWS sends the old devices for remanufacturing

- AWS sells the old devices to other hosting providers
- AWS destroys the old devices in accordance with industry-standard practices
(Correct)
- AWS stores the old devices in a secure place

Explanation

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. AWS uses specific techniques to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

References:

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

Question 49:

Skipped

What are the benefits of implementing a tagging strategy for AWS resources?
(Choose TWO)

- Track API calls in your AWS account
- Quickly identify software solutions on AWS
- Quickly identify resources that belong to a specific project

(Correct)

-

Track AWS spending across multiple resources

(Correct)

-

Quickly identify deleted resources and their metadata

Explanation

Amazon Web Services (AWS) allows customers to assign metadata to their AWS resources in the form of tags. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. Although there are no inherent types of tags, they enable customers to categorize resources by purpose, owner, environment, or other criteria. An effective tagging strategy will give you improved visibility and monitoring, help you create accurate chargeback/showback models, and get more granular and precise insights into usage and spend by applications and teams.

The other options are incorrect:

"Track API calls in your AWS account" is incorrect. AWS CloudTrail is the service that can be used to track API calls in your AWS account.

"Quickly identify deleted resources and their metadata" is incorrect. You cannot use tags to find deleted resources. Also, once you delete a resource, all its metadata will be deleted with it.

"Quickly identify software solutions on AWS" is incorrect. The AWS marketplace is the service that allows you to search for software solutions on AWS.

References:

<https://docs.aws.amazon.com/aws-technical-content/latest/cost-optimization-laying-the-foundation/tagging.html>

Question 50:

Skipped

What are the benefits of using an AWS-managed service? (Choose TWO)

-

Eliminates the need to encrypt data

-

Allows developers to control all patching related activities

-

Lowers operational complexity

(Correct)

-

Allows customers to deliver new solutions faster

(Correct)

-

Provides complete control over the virtual infrastructure

Explanation

AWS services that are managed lower operational complexity by automating time-consuming administration tasks such as hardware provisioning, software setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, security and compatibility they need. Because these services are instantly available to developers, they reduce dependency on in-house specialized skills and allow organizations to deliver new solutions faster.

The other options are incorrect:

"Provides complete control over the virtual infrastructure" is incorrect. When using a managed service you don't have complete control of it. You are limited in what you can do with it. For example, Amazon RDS limits you to six database engines to choose from. However, Amazon EC2 allows you to install and run any database.

"Allows developers to control all patching related activities" is incorrect. For managed services, patching activities are managed by AWS.

"Eliminates the need to encrypt data" is incorrect. It is always the customer's responsibility to encrypt data.

References:

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

Question 51:

Skipped

A company uses AWS Organizations to manage all of its AWS accounts. Which of the following allows the company to restrict what services and actions are allowed in each individual account?

- IAM Principals
- IAM policies
- AWS Service Control Policies (SCPs)

(Correct)

- AWS Fargate

Explanation

AWS Organizations provides central governance and management across multiple AWS accounts. AWS Service Control Policies (or AWS Organizations Policies) are a type of organization policy that you can use to manage permissions for all accounts in your organization. SCPs offer central control over the maximum available permissions for all member accounts in your organization. SCPs help you to ensure member accounts stay within your organization's access control guidelines. In SCPs, you can restrict which AWS services, resources, and individual API actions the users and roles in each member account can access. When AWS Organizations blocks access to a service, resource, or API action for a member account, a user or role in

that account cannot access it. This block remains in effect even if an administrator of a member account explicitly grants such permissions in an IAM policy.

Additional information:

What is the difference between an AWS Organizations service control policy (SCP) and an IAM policy?

An IAM policy provides granular control over what users and roles in individual accounts can do. AWS Organizations expands that control to the account level by giving you control over what users and roles in an account or a group of accounts can do. The resulting permissions are the logical intersection of what is allowed by AWS Organizations at the account level and the permissions that are explicitly granted by IAM at the user or role level within that account. In other words, the user can access only what is allowed by both the AWS Organizations policies and IAM policies. If either blocks an operation, the user can't access that operation. For example, if an SCP applied to an account states that the only actions allowed are Amazon EC2 actions, and the permissions on a principal (IAM user or role) in the same AWS account allow both EC2 actions and Amazon S3 actions, the principal is able to access only the EC2 actions.

The other options are incorrect:

"IAM Policies" is incorrect. IAM Policies cannot be used to manage access across multiple AWS accounts. An IAM Policy provides granular control over what users and roles in an **individual account** can do.

"IAM Principals" is incorrect. IAM Principles cannot be used to manage access across multiple AWS accounts. A principal is a person or application that can make a request for an action or operation on an AWS resource. The principal is authenticated as the AWS account root user or an IAM entity (users and roles) to make requests to AWS. Permissions in the IAM policies determine whether the request is allowed or denied.

"AWS Fargate" is incorrect. AWS Fargate is a serverless compute engine for Amazon Elastic Container Service (Amazon ECS) that allows customers to run containers without having to manage servers or clusters.

References:

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

Question 52:

Skipped

As part of the AWS Migration Acceleration Program (MAP), what does AWS provide to accelerate Enterprise adoption of AWS? (Choose TWO)

-

AWS Professional Services

(Correct)

-

AWS Artifact

-

Amazon PinPoint

-

Amazon Athena

-

AWS Partners

(Correct)

Explanation

AWS has helped thousands of organizations, including enterprises such as GE, the Coca-Cola Company, BP, Enel, Samsung, NewsCorp, and Twenty-First Century Fox, migrate to the cloud and free-up resources by lowering IT costs while improving productivity, operational resiliency, and business agility. The AWS Migration Acceleration Program (MAP) is designed to help enterprises that are committed to a migration journey achieve a range of these business benefits by migrating existing workloads to Amazon Web Services. MAP has been created to provide consulting support, training and services credits to reduce the risk of migrating to the cloud, build a strong operational foundation and help offset the initial cost of migrations. It includes a migration methodology for executing legacy migrations in a methodical

way as well as robust set of tools to automate and accelerate common migration scenarios.

By migrating to AWS, enterprises will be able to focus on business innovation instead of dedicating time and attention to maintaining their existing systems and technical debt. Sacrifices and painful trade-offs no longer have to be made to get something to market quickly. Instead, enterprises can focus on differentiating their business in the marketplace and taking advantage of new capabilities. By building the foundation to operate mission critical workloads on AWS, you will build capabilities that can be leveraged across a variety of projects. AWS have a number of resources to support and sustain your migration efforts including an experienced partner ecosystem to execute migrations, AWS Professional Services team to provide best practices and prescriptive advice and a training program to help IT professionals understand and carry out migrations successfully.

The other options are incorrect:

"Amazon Athena" is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. AWS customers can also use an Amazon S3 feature called **S3 Select** to query data on S3 using SQL commands; however, S3 Select can only be used to perform simple SQL queries on a single S3 Object.

"Amazon PinPoint" is incorrect. Amazon PinPoint is used to engage your customers by sending them targeted and transactional email, SMS, push notifications, and voice messages.

"AWS Artifact" is incorrect. AWS Artifact is a no cost, self-service portal for on-demand access to AWS' compliance reports.

References:

<https://aws.amazon.com/migration-acceleration-program/>

Question 53:

Skipped

Both AWS and traditional IT distributors provide a wide range of virtual servers to meet their customers' requirements. What is the name of these virtual servers in AWS?

- Amazon EBS Snapshots
- Amazon VPC
- Amazon EC2 Instances

(Correct)

- AWS Managed Servers

Explanation

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate them from common failure scenarios.

The other options are incorrect:

"Amazon VPC" is incorrect. Amazon VPC is used to create virtual networks in the cloud.

"AWS Managed Servers" is incorrect. Amazon EC2 instances are not managed by AWS. It is the responsibility of the customer to manage almost everything related to their instances.

"Amazon EBS Snapshots" is incorrect. Amazon EBS Snapshots are copies (backups) of EBS volumes.

References:

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

Question 54:

Skipped

Which AWS service or feature can be used to call AWS Services from different programming languages?

- AWS Management Console
- AWS CodeDeploy
- AWS Software Development Kit
- (Correct) AWS Command Line Interface

Explanation

The AWS Software Development Kit (AWS SDK) can simplify using AWS services in your applications with an API tailored to your programming language or platform. Programming languages supported include Java, .NET, Node.js, PHP, Python, Ruby, Go, and C++.

The other options are incorrect:

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

"AWS Management Console" is incorrect. AWS management Console allows you to manage AWS services through a web-based user interface.

"AWS Command Line Interface" is incorrect. AWS Command Line Interface (AWS CLI) allows you to control multiple AWS services from the command line and automate them through scripts NOT from programming languages.

References:

<https://aws.amazon.com/getting-started/tools-sdks/>

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

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

Question 55:

Skipped

What is one benefit and one drawback of buying a reserved EC2 instance? (Select TWO)

-

Reserved instances provide a significant discount compared to on-demand instances

(Correct)

-

There is no additional charge for using dedicated instances

-

Reserved instances require at least a one-year pricing commitment

(Correct)

- Reserved instances are best suited for periodic workloads
- Instances can be shut down by AWS at any time with no notification

Explanation

Amazon EC2 Reserved Instances (RI) provide a significant discount (up to 75%) compared to On-Demand pricing. Reserved instances can be purchased for a 1-year or 3-year term so you are committing to pay for them throughout this time period even if you don't use them.

The other options are incorrect:

"Reserved instances are best suited for periodic workloads" is incorrect. Reserved instances are not suitable for periodic workloads. You should use On-Demand instances instead.

"There is no additional charge for using dedicated instances" is incorrect. Dedicated instances are a different EC2 option.

"Instances can be shut down by AWS at any time with no notification" is incorrect. AWS can interrupt Spot Instances ;not reserved instances. Spot Instances can be shut down by AWS when the Spot price exceeds the maximum price, when the demand for Spot Instances rises, or when the supply of Spot Instances decreases.

References:

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

Question 56:

Skipped

Which support plan includes AWS Support Concierge Service?

- Business Support
- Standard Support
- Enterprise Support
(Correct)
- Premium Support

Explanation

Support Concierge is only available for the AWS Enterprise support plan. The Concierge Team are AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries, and work with you to implement billing and account best practices so that you can focus on what matters: running your business.

References:

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

Question 57:

Skipped

A company is planning to migrate a database with high read/write activity to AWS. What is the best storage option to use?

- Amazon EBS
(Correct)
- Amazon S3

- ○
Amazon Glacier
- ○
AWS Storage Gateway

Explanation

Databases require high read \ write performance and as such Amazon EBS is the correct answer. Amazon EBS volumes offer consistent and low-latency performance compared to other storage options. 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.

The other options are incorrect:

"Amazon Glacier" is incorrect. Amazon Glacier is a long-term object-level data storage.

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

"Amazon S3" is incorrect. Amazon S3 is an object-level storage, not block-level storage. Object storage is not suited for use in a high read/write scenarios because of performance limitations. In contrast, Amazon EBS is a block-level storage that provides an extremely high performance compared to Amazon S3. Amazon S3 is well suited for storing static assets such as photos and videos, backups, and log files.

References:

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

Question 58:

Skipped

Which AWS service can be used to send promotional text messages (SMS) to more than 200 countries worldwide?

-
-

Amazon Simple Notification Service (Amazon SNS)

(Correct)

-
-

Amazon Simple Storage Service (Amazon S3)

-
-

Amazon Simple Email Service (Amazon SES)

-
-

Amazon Simple Queue Service (Amazon SQS)

Explanation

Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. The A2P functionality enables you to send messages to users at scale via SMS, mobile push, and email.

Amazon SNS enables you to send messages or notifications directly to users with SMS text messages to over 200 countries. Additionally, you can mark your SMS messages as Transactional to optimize for reliable delivery, or you can mark them as Promotional to optimize for cost savings. SMS messages that carry marketing messaging should be marked Promotional. Amazon SNS ensures that promotional messages are sent over routes that have reasonable delivery reliability but are substantially cheaper than the most reliable routes.

The other options are incorrect:

"Amazon Simple Email Service (Amazon SES)" is incorrect. Amazon SES can only be used to send **emails**, not text (SMS) messages. Amazon SES is a cloud-based email sending service designed to help digital marketers and application developers send marketing, notification, and transactional emails.

"Amazon Simple Queue Service (Amazon SQS)" is incorrect. Amazon SQS is a highly reliable message queuing service that enables asynchronous message-based communication between distributed components of an application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

"Amazon Simple Storage Service" is incorrect. Amazon Simple Storage Service (Amazon S3) is an object storage service.

References:

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

Question 59:

Skipped

A company has hundreds of VPCs in multiple AWS Regions worldwide. What service does AWS offer to simplify the connection management among the VPCs?

-
- Amazon Connect
-
- Security Groups
-
- VPC Peering
-
- AWS Transit Gateway

(Correct)

Explanation

AWS Transit Gateway is a network transit hub that simplifies how customers interconnect all of their VPCs, across thousands of AWS accounts and into their on-premises networks. Customers can easily and quickly connect into a single centrally-

managed gateway, and rapidly growing the size of their network. Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. This hub and spoke model significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network. Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other network that is connected to the Transit Gateway. This ease of connectivity makes it easy to scale networks as business grow.

The other options are incorrect:

"VPC Peering" is incorrect. A VPC peering connection is a networking connection between **two** VPCs that enables customers to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. Using VPC peering to connect hundreds of VPCs is very complex and time consuming because customers need to peer each Amazon VPC to each other manually.

With AWS Transit Gateway, each VPC only has to connect to the Transit Gateway and not to every other VPC. Customers simply connect each Amazon VPC to the AWS Transit Gateway, and the Gateway will route traffic to and from each VPC.

"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.

"Security Groups" is incorrect. Security Groups are not used to connect Amazon VPCs. Security Groups are an Amazon VPC networking feature that allows customers to control instance traffic.

References:

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

Question 60:

Skipped

What are the benefits of using DynamoDB? (Choose TWO)

-

Supports the most popular NoSQL database engines such as CouchDB and MongoDB

-

Supports both relational and non-relational data models

-

Automatically scales to meet required throughput capacity

(Correct)

-

Offers extremely low (single-digit millisecond) latency

(Correct)

-

Provides resizable instances to match the current demand

Explanation

Benefits of DynamoDB include:

1- Performance at scale:

DynamoDB supports some of the world's largest scale applications by providing consistent, single-digit millisecond response times at any scale. You can build applications with virtually unlimited throughput and storage.

2- Serverless:

With DynamoDB, there are 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.

3- Highly available:

Availability and fault tolerance are built in, eliminating the need to architect your applications for these capabilities.

The other options are incorrect:

"Supports the most popular NoSQL database engines such as CouchDB and MongoDB" is incorrect. DynamoDB does not use or support any other NoSQL database engines. You only have access to DynamoDB's built-in engine.

"Supports both relational and non-relational data models" is incorrect. DynamoDB only supports the non-relational data model.

"Provides resizable instances to match the current demand" is incorrect. DynamoDB does not provide instances (servers). 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.

References:

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

Question 61:

Skipped

Which design principles relate to performance efficiency in AWS? (Choose TWO)

- Use serverless architectures

(Correct)

-

Enable audit logging

- Implement strong Identity and Access controls
- Build multi-region architectures to better serve global customers

(Correct)

- Apply security at all layers

Explanation

There are five design principles for performance efficiency in the cloud:

1- Democratize advanced technologies: Technologies that are difficult to implement can become easier to consume by pushing that knowledge and complexity into the cloud vendor's domain. Rather than having your IT team learn how to host and run a new technology, they can simply consume it as a service. For example, NoSQL databases, media transcoding, and machine learning are all technologies that require expertise that is not evenly dispersed across the technical community. In the cloud, these technologies become services that your team can consume while focusing on product development rather than resource provisioning and management.

2- Go global in minutes: Easily deploy your system in multiple Regions around the world with just a few clicks. This allows you to provide lower latency and a better experience for your customers at minimal cost.

3- Use serverless architectures: In the cloud, serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers, and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these managed services operate at cloud scale.

4- Experiment more often: With virtual and automatable resources, you can quickly carry out comparative testing using different types of instances, storage, or configurations.

5- Mechanical sympathy: Use the technology approach that aligns best to what you are trying to achieve. For example, consider data access patterns when selecting database or storage approaches.

Other options presented are related to security not performance.

References:

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

Question 62:

Skipped

A customer spent a lot of time configuring a newly deployed Amazon EC2 instance. After the workload increases, the customer decides to provision another EC2 instance with an identical configuration. How can the customer achieve this?

- By creating an AWS Config template from the old instance and launching a new instance from it
- By creating an EBS Snapshot of the old instance
- By installing Aurora on EC2 and launching a new instance from it
- By creating an AMI from the old instance and launching a new instance from it

(Correct)

Explanation

An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You must specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need. You can also launch instances from as many different AMIs as you need.

The other options are incorrect:

"By installing Aurora on EC2 and launching a new instance from it" is incorrect. Amazon Aurora is a database service. You cannot use it to launch EC2 instances. Also, you cannot install Aurora on EC2. Aurora is a managed service that is already installed on the AWS Cloud. You can launch Amazon Aurora using the Amazon RDS Management Console.

"By creating an EBS Snapshot of the old instance" is incorrect. Amazon EBS Snapshots are just backups for EBS volumes.

"By creating an AWS Config template from the old instance and launching a new instance from it" is incorrect. AWS Config is used to record and evaluate configurations of your AWS resources, and is not used to launch new instances.

References:

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

Question 63:

Skipped

Which of the below are responsibilities of the customer when using Amazon EC2?
(Choose TWO)

- Patching of the underlying infrastructure
- Setup and operation of managed databases
- Installing and configuring third-party software

(Correct)

-

Protecting sensitive data

(Correct)

-

Maintaining consistent hardware components

Explanation

Amazon EC2 requires the customer to perform all of the necessary security configuration and management tasks. When customers deploy Amazon EC2 instances, they are responsible for management of custom Amazon Machine Images, management of the guest operating systems (including updates and security patches), securing application access and data, installing and configuring third-party applications or utilities, and the configuration of the AWS-provided firewall (called a security group) on each instance.

The other options are incorrect:

"Patching of the underlying infrastructure" is incorrect. AWS is responsible for patching the underlying infrastructure. The customer is responsible for patching the operating system and any software or application run on EC2.

"Setup and operation of managed databases" is incorrect.

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

1- Using a managed database:

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

2- Installing a database software on Amazon EC2:

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

"Maintaining consistent hardware components" is incorrect. AWS is responsible for maintaining consistency of all hardware components.

References:

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

Question 64:

Skipped

Which of the following AWS services scale automatically without your intervention?
(Choose TWO)

-

Amazon EC2

-

AWS Lambda

(Correct)

-

Amazon EMR

-

Amazon S3

(Correct)

-

Amazon EBS

Explanation

Amazon S3 and Amazon EFS are storage services that scale automatically in storage capacity without any intervention to meet increased demand.

Also, AWS Lambda dynamically scales function execution in response to increased traffic.

The other options are incorrect:

Amazon EMR is incorrect. Amazon EMR doesn't scale on its own. You have to configure the AWS Auto Scaling feature to scale EMR automatically.

Amazon EC2 is incorrect. Amazon EC2 does scale automatically, but first you have to create an Auto Scaling system by creating a launch configuration, an auto scaling group, and determine the desired, minimum and maximum number of instances to provision.

Amazon EBS is incorrect. Amazon Elastic Block Store (Amazon EBS) provides persistent block level storage volumes for use with Amazon EC2 instances in the AWS Cloud.

References:

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

Question 65:

Skipped

A company plans to migrate a large amount of archived data to AWS. The archived data must be maintained for a period of 5 years and must be retrievable within 5 hours of a request. What is the most cost-effective AWS storage service to use?

-
- Amazon EBS Infrequent Access
-
- Amazon S3 Standard
-
- Amazon S3 Glacier

(Correct)

-

Amazon EFS Infrequent Access

Explanation

AWS Customers can use **Amazon S3 Glacier** or **Amazon S3 Glacier Deep Archive** to backup large amounts of data at very low costs.

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

Amazon S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class that supports long-term retention and digital preservation for data that may be accessed once or twice in a year.

Choosing between S3 Glacier and S3 Glacier Deep Archive depends on how quickly you must retrieve your data. With S3 Glacier, you can retrieve your data within **a few minutes to several hours (1-5 minutes to 12 hours)**, whereas with S3 Glacier Deep Archive, the minimum retrieval period is 12 hours.

The other options are incorrect:

"Amazon EFS Infrequent Access" is incorrect. Amazon Elastic File System (Amazon EFS) is not a cost-effective solution for data archiving. Amazon EFS is a **file** storage service for use with Amazon compute (EC2, containers, serverless) and on-premises servers. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances.

What is Amazon EFS Infrequent Access?

Amazon EFS Standard-Infrequent Access (EFS Standard-IA) and Amazon EFS One Zone-Infrequent Access (EFS One Zone-IA) are storage classes that provide price/performance that is cost-optimized for files not accessed every day, with storage prices **up to 92% lower** compared to Amazon EFS Standard (EFS Standard) and Amazon EFS One Zone (EFS One Zone) storage classes respectively. To get started with Infrequent Access (IA) storage classes, simply enable Amazon EFS Lifecycle Management for your file system by selecting a lifecycle policy that matches

your needs. Amazon EFS will automatically and transparently move your files to the lower cost regional EFS Standard-IA storage class or EFS One Zone-IA storage class based on the last time they were accessed. You don't have to worry about which of your files are actively used and which are infrequently accessed.

"Amazon EBS Infrequent Access" is incorrect. Amazon EBS is not a cost-effective solution for data archiving. Amazon EBS provides **block-level** storage volumes for use with Amazon EC2 and RDS instances. Amazon EBS does not offer storage tiers for less frequently accessed data. Infrequent Access storage tiers are available only for Amazon S3 and Amazon EFS.

"Amazon S3 Standard" is incorrect. Amazon S3 Standard is not a cost-effective solution for data archiving. Amazon S3 Standard is a general-purpose **object** storage for active, frequently accessed data with **millisecond access**. S3 Standard use cases include: cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

Additional information:

In S3, we can only host static websites, or **static assets of a dynamic website** (such as images, audio files, video files, etc.).

A dynamic website relies on server-side processing and it uses server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting and cannot be used to host dynamic websites. AWS has computing resources for hosting dynamic websites such as Amazon EC2 or Lambda.

References:

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

Question 1:

Skipped

An organization has a legacy application designed using monolithic-based architecture. Which AWS Service can be used to decouple the components of the application?

- Virtual Private Gateway
- Amazon SQS

(Correct)

- Amazon CloudFront
- AWS Artifact

Explanation

A monolithic application is designed to be self-contained; components of the application are interconnected and interdependent rather than loosely coupled as is the case with Microservices applications.

With monolithic architectures, all processes are **tightly-coupled** and run as a single service. This means that if one process of the application experiences a spike in demand, the entire architecture must be scaled. Adding or improving a monolithic application's features becomes more complex as the code base grows. This complexity limits experimentation and makes it difficult to implement new ideas. Monolithic architectures add risk for application availability because many dependent and tightly coupled processes increase the impact of a single process failure.

With a microservices architecture, an application is built as **loosely-coupled** components that run each application process as a service. These services communicate via a well-defined interface using lightweight APIs. Services are built for business capabilities and each service performs a single function. Because they are independently run, each service can be updated, deployed, and scaled to meet demand for specific functions of an application. Microservices architectures make applications easier to scale and faster to develop, enabling innovation and accelerating time-to-market for new features.

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

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

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

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

The other options are incorrect.

Virtual Private Gateway is incorrect. A virtual private gateway (VPG) is the VPN concentrator on the Amazon side of the VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the Site-to-Site VPN connection. AWS Virtual Private Network (AWS VPN) is one of the connectivity options that enables you to build hybrid cloud architectures by securely connecting your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC).

Amazon CloudFront is incorrect. Amazon CloudFront is a global content delivery network (CDN) service.

AWS Artifact is incorrect. AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements.

References:

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

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

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

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

Question 2:

Skipped

A customer is seeking to store objects in their AWS environment and to make those objects downloadable over the internet. Which AWS Service can be used to accomplish this?



Amazon EBS



Amazon EFS



Amazon Instance Store



Amazon S3

(Correct)

Explanation

Amazon S3 provides a simple web service interface that you can use to store and retrieve any amount of data, any time, from anywhere on the internet. Amazon S3 assigns a URL for each object you upload. URLs are used to download the objects you want at any time. Amazon S3 is the only AWS service that provides object level storage.

The other options are incorrect:

Amazon EFS is incorrect. Amazon Elastic File System (Amazon EFS) is not an object store. Amazon EFS is a shared NFS **file** storage system that scales automatically with use.

Amazon Elastic Block Store (EBS) is incorrect. Amazon Elastic Block Store (Amazon EBS) is not an object store. Amazon EBS is a **block** storage service that is used to create volumes for use with Amazon EC2 and Amazon RDS.

Amazon Instance Store is incorrect. Amazon EC2 Instance Store is not an object store. Amazon EC2 Instance Store provides ephemeral **block**-level storage that is physically attached to Amazon EC2 instances.

References:

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

Question 3:

Skipped

Which of the following is NOT a factor when estimating the costs of Amazon EC2? (Choose TWO)

-

Number of Hosted Zones

(Correct)

- The amount of time the instances will be running
- Allocated Elastic IP Addresses
- Number of security groups

(Correct)

- Number of instances

Explanation

There are no associated costs for "EC2 Security Groups" or "Hosted Zones" and thus are correct answers.

EC2 Security groups are free to use.

Hosted Zones are not free, but they are not related to Amazon EC2 costs. Hosted Zones is one of the factors of the Amazon Route 53 costs.

The other options represent factors you should consider when estimating the cost of Amazon EC2 and are therefore incorrect.

When you begin to estimate the cost of using Amazon EC2, consider the following:

1- Clock hours of server time: The amount of time that the instances will be running has a direct bearing on the overall price, as EC2 instances are charged either by the hour or by the second, depending on which AMI is used.

2- Instance type: Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity.

3- Pricing model: On-Demand, Reserved, Spot, Savings Plans, and Dedicated

4- Number of instances: You can provision multiple instances of your Amazon EC2 and Amazon EBS resources to handle peak loads.

5- Load balancing: The number of hours the Elastic Load Balancer runs and the amount of data it processes contribute to the EC2 monthly cost.

6- Elastic IP addresses: To ensure efficient use of Elastic IP addresses, AWS imposes a small hourly charge if an Elastic IP address is **not associated** with a running instance, or if it is **associated** with a stopped instance. While the instance is running, you are not charged for one Elastic IP address associated with the instance, but additional Elastic IPs are not free.

7- Operating systems and software packages: Operating system prices are included in instance prices, unless you choose to bring your own licenses.

References:

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/how-aws-pricing-works.pdf> page 10, 11

Question 4:

Skipped

Which AWS service or feature is used to manage the keys used to encrypt customer data?

-
-

AWS KMS

(Correct)

-
-

Amazon Macie

-
-

Multi-Factor Authentication (MFA)

• ○

AWS Service Control Policies (SCPs)

Explanation

AWS Key Management Service (AWS KMS) is a managed service that enables customers to easily create and control the keys used for cryptographic operations. The service provides a highly available key generation, storage, management, and auditing solution for customers to encrypt or digitally sign data within their applications or to control the encryption of data across AWS services.

The other options are incorrect:

"AWS Service Control Policies (SCPs)" is incorrect. AWS Service Control Policies (or AWS Organizations Policies) are a type of organization policy that you can use to manage permissions for all accounts in your organization. SCPs offer central control over the maximum available permissions for all member accounts in your organization. SCPs help you to ensure member accounts stay within your organization's access control guidelines. In SCPs, you can restrict which AWS services, resources, and individual API actions the users and roles in each member account can access. When AWS Organizations blocks access to a service, resource, or API action for a member account, a user or role in that account cannot access it. This block remains in effect even if an administrator of a member account explicitly grants such permissions in an IAM policy.

"Multi-Factor Authentication (MFA)" is incorrect. While MFA can help customers protect their data, MFA is not used to store or manage encryption keys.

"Amazon Macie" is incorrect. Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides customers with dashboards and alerts that give visibility into how this data is being accessed or moved. Amazon Macie is not a key management service.

References:

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

Question 5:

Skipped

A company is developing an application that will leverage facial recognition to automate photo tagging. Which AWS Service should the company use for facial recognition?

- Amazon Rekognition
- **(Correct)**
- AWS IAM
- Amazon Comprehend
- Amazon Polly

Explanation

Amazon Rekognition is a service that makes it easy to add image analysis to your applications. With Rekognition, you can detect objects, scenes, and faces in images. You can also search and compare faces. The Amazon Rekognition API enables you to quickly add sophisticated deep-learning-based visual search and image classification to your applications.

The other options are incorrect:

"Amazon Comprehend" is incorrect. Amazon Comprehend is a **Natural Language Processing (NLP) service** that uses machine learning to find meaning and insights in text. Customers can use Amazon Comprehend to identify the language of the text, extract key phrases, places, people, brands, or events, understand sentiment about products or services, and identify the main topics from a library of documents. The source of this text could be web pages, social media feeds, emails, or articles.

Amazon Comprehend is fully managed, so there are no servers to provision, and no machine learning models to build, train, or deploy.

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

"Amazon Polly" is incorrect. Amazon Polly is a service that turns text into lifelike speech.

"AWS IAM" is incorrect. AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely.

References:

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf> page 35

Question 6:

Skipped

What is the AWS Support feature that allows customers to manage support cases programmatically?



AWS Operations Support



AWS Personal Health Dashboard



AWS Support API

(Correct)



AWS Trusted Advisor

Explanation

The AWS Support API provides programmatic access to AWS Support Center features to create, manage, and close support cases, and operationally manage Trusted Advisor check requests and status. AWS Support API is available only for AWS customers who have a **Business or Enterprise** support plan.

The service currently provides two different groups of operations:

- 1- Support Case Management operations to manage the entire life cycle of AWS support cases, from creating a case to resolving it.
- 2- Trusted Advisor operations to access the checks provided by AWS Trusted Advisor.

The other options are incorrect:

"AWS Trusted Advisor" is incorrect. AWS Trusted Advisor analyzes AWS environments and provides best practice recommendations in five categories: cost optimization, security, fault tolerance, performance and service limits (also referred to as Service quotas).

"AWS Personal Health Dashboard" is incorrect. AWS Personal Health Dashboard provides a view of the health of AWS services and resources that are used by a given AWS account.

"AWS Operations Support" is incorrect. Included with the Enterprise support plan, Operations Support provides consultative reviews of your AWS operations and advice for optimization.

References:

<https://docs.aws.amazon.com/awssupport/latest/user/Welcome.html>

Question 7:

Skipped

Which of the following Amazon RDS features facilitates offloading of database read activity?

- Automated Backups
- Multi-AZ Deployments
- Read Replicas

(Correct)

- Database Snapshots

Explanation

You can reduce the load on your source DB Instance by routing read queries from your applications to one or more read replicas. Read replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

The other options are incorrect:

"Automated Backups" is incorrect. The automated backup feature of Amazon RDS enables point-in-time recovery for your database instance. This allows you to restore your database instance to any second during the retention period.

Additional information: According to the AWS Shared Responsibility Model, Amazon RDS backups is the sole responsibility of AWS. Amazon RDS is an AWS-managed service, which means that AWS is responsible for everything related to backups, patching, recovery, failure detection, and repair.

"Multi-AZ Deployments" is incorrect. Multi-AZ Deployments are used to increase the fault tolerance of your application by automatically failing over to the standby DB instance which located in a separate AZ within the same region.

"Database Snapshots" is incorrect. Database snapshots are user-initiated backups of your RDS instance stored in Amazon S3 that are kept until you explicitly delete them.

References:

<https://aws.amazon.com/rds/details/read-relicas/>

Question 8:

Skipped

A company is using EC2 Instances to run their e-commerce site on the AWS platform. If the site becomes unavailable, the company will lose a significant amount of money for each minute the site is unavailable. Which design principle should the company use to minimize the risk of an outage?

Fault Tolerance

(Correct)

Least Privilege

Pilot Light

Multi-threading

Explanation

A system that is designed to be fault tolerant can recover gracefully from EC2 instance failures. Amazon Web Services gives customers access to a vast amount of IT infrastructure—compute, storage, and communications—that they can allocate automatically (or nearly automatically) to account for almost any kind of failure.

The other options are incorrect:

"Least Privilege" is incorrect. Principle of least privilege is a security concept related to access management, not fault tolerance. The principle of least privilege means granting users the required permissions to perform the tasks entrusted to them and nothing more.

"Pilot Light" is incorrect. A pilot light scenario is a disaster recover / business continuity scenario wherein a minimal amount of services are kept running in a failover location to enable the business to meet their Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in the event of a disaster. By nature, a pilot light scenario will take some time to spin up and promote to production (as opposed to an active-active DR scenario) and will therefore not mitigate the per-minute losses that will be experienced by the company in the event of an outage.

Additional information: Recovery time objective (RTO) and recovery point objective (RPO) are two key metrics to consider when developing a disaster recover (DR) plan. RTO represents how many hours it takes customers to return to a working state after a disaster. RPO, which is also expressed in hours, represents how much data customers could lose when a disaster happens. For example, an RPO of 1 hour means that customers could lose up to 1 hour's worth of data when a disaster occurs.

Read more about disaster recovery scenarios here:

<https://aws.amazon.com/blogs/publicsector/rapidly-recover-mission-critical-systems-in-a-disaster/>

"Multi-threading" is incorrect. Multi-threading is the ability of a central processing unit (CPU) to provide multiple threads of execution concurrently, which may lead to faster overall execution. Amazon EC2 instances support multi-threading. For example, an m5.xlarge instance type has two CPU cores and two threads per core by default—four threads in total. While multi-threading leads to maximum utilization of the CPU and improves the overall performance of EC2 instances, multi-threading has nothing to do with recovering EC2 instances from failures.

References:

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/wellarchitected-reliability-pillar.pdf#design-your-workload-to-withstand-component-failures>

Question 9:

Skipped

Which AWS service enables you to quickly purchase and deploy SSL/TLS certificates?

- Amazon GuardDuty
 - AWS ACM
- (Correct)**
- Amazon Detective
 - AWS WAF

Explanation

AWS Certificate Manager (AWS ACM) 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. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks.

AWS Certificate Manager removes many of the time-consuming and error-prone steps to acquire an SSL/TLS certificate for your website or application. With a few clicks in the AWS Management Console, you can request a trusted SSL/TLS certificate from AWS. Once the certificate is created, AWS Certificate Manager takes care of deploying certificates to help you enable SSL/TLS for your website or application.

The other options are incorrect:

"AWS WAF" is incorrect. AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define.

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

"Amazon Detective" is incorrect. Amazon Detective is a security service that makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities.

Additional information:

How does Amazon Detective differ from Amazon GuardDuty?

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

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

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

References:

Question 10:

Skipped

A key practice when designing solutions on AWS is to minimize dependencies between components so that the failure of a single component does not impact other components. What is this practice called?

-

Loosely coupling

(Correct)

-

Scalable coupling

-

Elastic coupling

-

Tightly coupling

Explanation

The concept of loosely coupling an application refers to breaking the application into components that perform aspects of a task independently of one another. Using this design concept minimizes the risk that a change or a failure in one component will impact other components.

References:

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

Question 11:

Skipped

Which of the following are advantages of using AWS as a cloud computing provider? (Choose TWO)

-

Manages all the compliance and auditing tasks

- Eliminates the need to monitor servers and applications
- Enables customers to trade their capital expenses for operational expenses

(Correct)

- Eliminates the need to guess on infrastructure capacity needs

(Correct)

- Provides custom hardware to meet any specification

Explanation

Advantages of Cloud Computing include: (IMPORTANT)

1- Trade capital for variable expense: Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can only pay when you consume computing resources, and only pay for how much you consume. By using AWS, infrastructure costs are converted to a pay-as-you-go model, where customers are charged for the resources that they consume, and those costs are incurred as operating costs instead of as capital expenditures.

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

3- Stop guessing capacity: Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often either end up sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little as you need, and scale up and down as required with only a few minutes notice.

4- Increase speed and agility: In a cloud computing environment, new IT resources are only ever a click away, which means you reduce the time it takes to make those resources available to your developers from weeks to just minutes. This results in a

dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

5- Stop spending money on running and maintaining data centers: Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking and powering servers.

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

The other options are incorrect:

"Eliminates the need to monitor servers and applications" is incorrect. Using AWS does not eliminate the need to monitor servers and applications. Monitoring servers and applications remains the responsibility of the customer.

"Manages all the compliance and auditing tasks" is incorrect. Security and Compliance is a shared responsibility between AWS and the customer. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards. Examples of the assurance programs with which AWS complies include SOC, PCI DSS Level 1, ISO 9001, and ISO 27001. AWS customers remain responsible for complying with applicable compliance laws and regulations.

"Provides custom hardware to meet any specification" is incorrect. AWS doesn't provide hardware. AWS provides Cloud Computing services.

References:

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

Question 12:

Skipped

Which of the following are types of AWS Identity and Access Management (IAM) identities? (Choose TWO)

-

IAM Roles

(Correct)

-

AWS Organizations

-

IAM Users

(Correct)

-

IAM Policies

-

AWS Resource Groups

Explanation

Identities on AWS include users (or groups) and roles. Customers create these identities on AWS to manage access to AWS resources and determine the actions that each identity can perform on those resources.

IAM Roles:

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, applications or services that normally don't 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. 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:

An 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. 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 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 EC2.

The other options are incorrect:

"AWS Organizations" is incorrect. AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.

"IAM Policies" is incorrect. IAM policies let you allow or deny access to AWS services (such as Amazon S3), individual AWS resources (such as a specific S3 bucket), or individual API actions (such as s3:CreateBucket). An IAM policy can be applied only to IAM users, groups, or roles, and it can never restrict the root identity of the AWS account (The AWS root account). It is important to note that while IAM Policies are used by IAM Identities, the policy itself is not a form of IAM Identity.

"AWS Resource Groups" is incorrect. Resource Groups are a way to manage multiple resources (such as EC2 instances, S3 buckets, ...) as a group rather than move from one AWS service to another for each task.

References:

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

Question 13:

Skipped

The TCO gap between AWS infrastructure and traditional infrastructure has widened over the recent years. Which of the following could be the reason for that?

- AWS helps customers invest more in capital expenditures
- AWS continues to lower the cost of cloud computing for its customers

(Correct)

- AWS secures AWS resources at no additional charge
- AWS automates all infrastructure operations, so customers save more on human resources costs

Explanation

AWS continues to lower the cost of cloud computing for its customers, making everything from web apps to big data on AWS even more cost-effective and widening the TCO (Total Cost of Ownership) gap with traditional infrastructure. Since 2014, AWS has reduced the cost of compute by an average of 30%, storage by an average of 51% and relational databases by an average of 28%.

The other options are incorrect:

"AWS automates all infrastructure operations, so customers save more on human resources costs" is incorrect. AWS does not automate all infrastructure operations. While certain AWS Services, such as RDS, are fully managed services, other aspects of infrastructure management, such as Amazon EC2 remain the responsibility of the customer.

"AWS helps customers invest more in capital expenditures" is incorrect. AWS reduces the need to invest in large capital expenditures and provides a pay-as-you-go model that empowers its customers to invest in the capacity they need and use it only when the business requires it.

"AWS secures AWS resources at no additional charge" is incorrect. Securing AWS resources is a shared responsibility between AWS and its customers. Additionally, some AWS security services and features have an associated cost.

References:

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

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

Question 14:

Skipped

Which AWS Service provides integration with Chef to automate the configuration of EC2 instances?

-
-

AWS CloudFormation

-
-

AutoScaling

-
-

AWS Config



AWS OpsWorks

(Correct)

Explanation

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.

The other options are incorrect:

AWS CloudFormation is incorrect. AWS CloudFormation allows customers to provision infrastructure as code.

AutoScaling is incorrect. AutoScaling is used to increase or decrease capacity based on demand.

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

References:

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

Question 15:

Skipped

Which of the following factors should be considered when determining the region in which AWS Resources will be deployed? (Choose TWO)



Cost

(Correct)

- The AWS Region's security level
- Data sovereignty

(Correct)

- Geographic proximity to the company's location
- The planned number of VPCs

Explanation

Per AWS Best Practices, proximity to your end users, regulatory compliance, data residency constraints, and cost are all factors you have to consider when choosing the most suitable AWS Region.

The other options are incorrect:

"The planned number of VPCs" is incorrect. The number of VPCs a customer can have in a given region is the same irrespective of which AWS Region the customer is using.

"The AWS Region's security level" is incorrect. The level of security is almost identical for all AWS regions.

"Geographic proximity to the company's location" is incorrect. To achieve the lowest network latency and the quickest response, the best practice is to choose the closest AWS region to the end-users (**not to the company's location**). For example, if an application is developed in Japan but is primarily accessed by users in North America, the customers will have a better experience (lower application latency) if the

application is deployed to AWS Regions in North America than if it were deployed to the Tokyo Region.

References:

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

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

Question 16:

Skipped

Which AWS Service offers volume discounts based on usage?



Amazon VPC



Amazon Lightsail



Amazon S3

(Correct)



AWS Cost Explorer

Explanation

Some AWS services are priced in *tiers*, which specify unit costs for defined amounts of AWS usage. As your usage increases, your usage crosses thresholds into new pricing tiers that specify lower unit costs for additional usage in a month. For example, the more Amazon S3 capacity a customer uses, the lower the cost per unit volume.

The current S3 pricing for the us-east-1 region is:

1st tier: \$0.023 per GB / month for the first 50 TB stored

2nd tier: \$0.022 per GB / month for the next 450 TB stored

3rd tier: \$0.021 per GB / month for all storage consumed above 500 TB.

Additional information:

Using [consolidated billing](#), customers can combine usage from multiple AWS accounts into a single invoice, allowing them to reach the tiers with lower prices faster.

References:

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

Question 17:

Skipped

A company wants to grant a new employee long-term access to manage Amazon DynamoDB databases. Which of the following is a recommended best-practice when granting these permissions?

- Create an IAM **user** and attach a policy with Administrator access permissions
- Create an IAM **user** and attach a policy with Amazon DynamoDB access permissions

(Correct)

- Create an IAM **role** and attach a policy with Amazon DynamoDB access permissions
- Create an IAM **role** and attach a policy with Administrator access permissions

Explanation

IAM user is the recommended IAM entity when granting a person long-term access permission. After you create an IAM user, you attach a policy that defines what he or she can and cannot do in AWS. When creating this policy, you should follow the principle of least privilege. The principle of least privilege ensures only the required permissions are granted, nothing more.

The new employee only needs permission to access and manage Amazon DynamoDB databases. Therefore, the option that says "Create an IAM user and attach a policy with Amazon DynamoDB access permissions" is the correct answer.

The other options are incorrect:

"Create an IAM user and attach a policy with Administrator Access permissions" and "Create an IAM role and attach a policy with Administrator access permissions" are incorrect. Administrator Access provides full access to AWS services and resources. This option contradicts the principle of least privilege. The principle of least privileges means granting users the required permissions to perform the tasks entrusted to them and nothing more.

"Create an IAM role and attach a policy with Amazon DynamoDB access permissions" is incorrect. 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.

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.

References:

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

Question 18:

Skipped

What should you do if you see resources, which you don't remember creating, in the AWS Management Console? (Choose TWO)

-

Open an investigation and delete any potentially compromised IAM users

(Correct)

-

Change your AWS root account password and the passwords of any IAM users

(Correct)

-

Stop all running services and open an investigation

-

Give your root account password to AWS Support so that they can assist in troubleshooting and securing the account

-

Check the AWS CloudTrail logs and delete all IAM users that have access to your resources

Explanation

If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the following tasks:

- 1- Change your AWS root account password and the passwords of all IAM users.
- 2- Delete or rotate all root and AWS Identity and Access Management (IAM) access keys.
- 3- Delete any potentially compromised IAM users.
- 4- Delete any resources on your account you didn't create, such as EC2 instances and AMIs, EBS volumes and snapshots, and IAM users.

5- Respond to any notifications you received from AWS Support through the AWS Support Center.

The other options are incorrect:

"Give your root account password to AWS Support so that they can assist in troubleshooting and securing the account" is incorrect. While AWS support can assist in troubleshooting and securing the account, customers should NOT give their root account password to AWS Support (or anyone) for any reason.

"Check the AWS CloudTrail logs and delete all IAM users that have access to your resources" is incorrect. It is a good idea to check the CloudTrail logs that are aggregated recently, however you should not delete all IAM users that have access to your resources. Doing so, will break all the relationships and permissions you have made and may bring down all systems in your account. Instead, you should open an investigation, check the AWS CloudTrail logs, and delete all potentially compromised IAM users.

"Stop all running services, and open an investigation" is incorrect. Stopping all running services is not required when investigating such issues.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/potential-account-compromise/>

Question 19:

Skipped

Which AWS Service offers an NFS file system that can be mounted concurrently from multiple EC2 instances?

-

Amazon Simple Storage Service

-
- Amazon Elastic File System

(Correct)

-
- AWS Storage Gateway
-
- Amazon Elastic Block Store

Explanation

Amazon Elastic File System (Amazon EFS) provides a fully managed **NFS file system** for use with AWS Cloud services and on-premises resources.

Amazon EFS supports the latest version of the Network File System (NFS) protocol, so the applications and tools that you use today work seamlessly with Amazon EFS. Multiple compute instances, including Amazon EC2, Amazon ECS, and AWS Lambda, can access an Amazon EFS file system at the same time, providing a common data source for workloads and applications running on more than one compute instance or server.

With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it.

The other options are incorrect:

"AWS Storage Gateway" is incorrect. AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage.

"Amazon Elastic Block Store" is incorrect. An Amazon Elastic Block Store (Amazon EBS) volume can be attached to only one instance at a time.

"Amazon Simple Storage Service" is incorrect. Amazon Simple Storage Service (Amazon S3) is an object storage service, and cannot serve as a filesystem that is mounted to Amazon EC2 instances.

References:

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf> page 60

Question 20:

Skipped

There is a requirement to grant a DevOps team full administrative access to all resources in an AWS account. Who can grant them these permissions?

- AWS technical account manager
- AWS account owner **(Correct)**
- AWS cloud support engineers
- AWS security team

Explanation

The account owner is the entity that has complete control over all resources in their AWS account.

The other options are incorrect.

"AWS cloud support engineers" is incorrect. AWS cloud support engineers provide technical support to customers who are having issues with the system. Cloud support engineers are available only for the Business and Enterprise support plans.

"AWS technical account manager" is incorrect. AWS technical account manager (TAM) helps AWS customers craft and execute strategies to drive their adoption and use of AWS services. AWS TAM is available only for the Enterprise support plan.

AWS security team is incorrect. The AWS Security Team is an internal AWS team that is responsible for the security of services offered by AWS.

References:

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

Question 21:

Skipped

Which of the below options is true of Amazon Cloud Directory?

- Amazon Cloud Directory allows users to access AWS with their existing Active Directory credentials
- Amazon Cloud Directory allows the organization of hierarchies of data across multiple dimensions

(Correct)

- Amazon Cloud Directory allows for registration and management of domain names
- Amazon Cloud Directory enables the analysis of video and data streams in real time

Explanation

Amazon Cloud Directory is a cloud-native, highly scalable, high-performance directory service that provides web-based directories to make it easy for you to

organize and manage all your application resources such as users, groups, locations, devices, and policies, and the rich relationships between them.

Unlike existing traditional directory systems, Cloud Directory does not limit organizing directory objects in a single fixed hierarchy. In Cloud Directory, you can organize directory objects into multiple hierarchies to support multiple organizational pivots and relationships across directory information. For example, a directory of users may provide a hierarchical view based on reporting structure, location, and project affiliation. Similarly, a directory of devices may have multiple hierarchical views based on its manufacturer, current owner, and physical location. With Cloud Directory, you can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries.

The other options are incorrect:

"Amazon Cloud Directory allows users to access AWS with their existing Active Directory credentials" is incorrect. Amazon Cloud Directory [and AWS Directory Service](#) are two different services. AWS Directory Service is the service that provides single sign-on (SSO) to applications and services on AWS. AWS Directory Service uses secure Windows trusts to enable users to sign in to the AWS Management Console and the AWS Command Line Interface (CLI) using their existing corporate Microsoft Active Directory credentials.

"Amazon Cloud Directory enables the analysis of video and data streams in real time" is incorrect. The AWS Service that enables the analysis of video and data streams in real time is Amazon Kinesis.

"Amazon Cloud Directory allows for registration and management of domain names" is incorrect. Amazon Route 53 is the AWS Service that allows for registration and management of domain names.

References:

<https://aws.amazon.com/cloud-directory/>

Question 22:

Skipped

Which of the following AWS offerings are serverless services? (Choose TWO)

-

Amazon DynamoDB

(Correct)

-

Amazon EC2

-

Amazon EMR

-

AWS Lambda

(Correct)

-

Amazon RDS

Explanation

AWS Lambda is a compute service that lets customers run code without provisioning or managing servers. AWS Lambda executes code only when needed and scales automatically, from a few requests per day to thousands per second.

With DynamoDB, there are 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.

AWS Serverless Services include:

Compute: AWS Lambda, AWS Fargate

Messaging: Amazon SNS, Amazon SQS

Database: Amazon DynamoDB, Amazon Aurora Serverless

Orchestration: AWS Step Functions

The other options are incorrect:

Amazon EC2 is incorrect. Amazon EC2 provides its compute capacity through instances (servers). Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications.

Amazon RDS is incorrect. Amazon RDS also provides its compute capacity through instances (servers). Amazon RDS provides a selection of instance types optimized to fit different relational database use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your database.

Amazon EMR is incorrect. Amazon EMR is a web service that uses Amazon EC2 instances (servers) to enable businesses, researchers, data analysts, and developers to process vast amounts of data easily and cost-efficiently.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

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

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

Question 23:

Skipped

Which of the following are examples of AWS-managed databases? (Choose TWO)

-

Amazon Neptune

(Correct)

- MySQL on Amazon EC2
- Amazon CloudSearch
- Amazon RDS for MySQL

(Correct)

- Microsoft SQL Server on Amazon EC2

Explanation

AWS-managed databases are a database as a service offering from AWS where AWS manages the underlying hardware, storage, networking, backups, and patching. Users of AWS-managed databases simply connect to the database endpoint, and do not have to concern themselves with any aspects of managing the database. Examples of AWS-managed databases include: Amazon RDS (Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and Microsoft SQL Server), Amazon Neptune, Amazon DocumentDB, Amazon Redshift, and Amazon DynamoDB.

Amazon Neptune is a fully-managed **graph database service** that makes it easy to build and run applications that work with highly connected datasets, such as social networking, recommendation engines, and knowledge graphs. Amazon Neptune is fully managed and handles the time-consuming tasks such as provisioning, patching, backup, recovery, failure detection and repair.

Amazon RDS for MySQL is a managed service that makes it easy to set up, operate, and scale a **MySQL database** in the cloud. Amazon RDS for MySQL frees you up to focus on application development by managing time-consuming database administration tasks including backups, software patching, monitoring, scaling and replication.

The other options are incorrect:

"Microsoft SQL Server on Amazon EC2" and "MySQL on Amazon EC2" are incorrect. Microsoft SQL Server on Amazon EC2 and MySQL on Amazon EC2 are customer-managed databases, not AWS-managed databases. Any database that is running on EC2 is managed by the customer, and not by AWS.

Note: Customers can install and run any database engine - or any Software - on Amazon EC2, but in this case, the customer is responsible for managing the software, not AWS.

"Amazon CloudSearch" is incorrect. Amazon CloudSearch is a managed service in the AWS Cloud that makes it simple and cost-effective to set up, manage, and scale a search solution for your website or application.

References:

<https://aws.amazon.com/neptune/getting-started/>

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

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

<https://aws.amazon.com/rds/mysql/what-is-mysql/>

Question 24:

Skipped

Which of the following are true regarding the languages that are supported on AWS Lambda? (Choose TWO)

-

Lambda doesn't support programming languages; it is a serverless compute service

-

Lambda natively supports a number of programming languages such as Node.js, Python, and Java

(Correct)

-

Lambda only supports Python and Node.js, but third party plugins are available to convert code in other languages to these formats

-

Lambda is AWS' proprietary programming language for microservices

-

Lambda can support any programming language using an API

(Correct)

Explanation

AWS Lambda natively supports Java, Go, PowerShell, Node.js, C#, Python, and Ruby code, and provides a Runtime API which allows customers to use any additional programming languages to author their functions.

The other options are incorrect:

"Lambda only supports Python and Node.js, but third party plugins are available to convert code in other languages to these formats" is incorrect. AWS supports many languages natively, including Go, PowerShell, Ruby, and C#. Additionally, there are no third-party plugins that will convert code from one language to another.

"Lambda doesn't support programming languages; it is a serverless compute service" is incorrect. AWS Lambda is a serverless compute service that lets customers run code written using their preferred programming language.

"Lambda is AWS' proprietary programming language for microservices" is incorrect. Lambda is not a programming language; It allows customers to run code without provisioning or managing servers.

References:

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

Question 25:

Skipped

What are the advantages of using Auto Scaling Groups for EC2 instances?

-
- Auto Scaling Groups scales EC2 instances in multiple Availability Zones to increase application availability and fault tolerance
- (Correct)**
-
- Auto Scaling Groups distributes application traffic across multiple Availability Zones to enhance performance
-
- Auto Scaling Groups caches the most recent responses at global edge locations to reduce latency and improve performance
-
- Auto Scaling Groups scales EC2 instances across multiple regions to reduce latency for global users

Explanation

Amazon EC2 Auto Scaling offers the following benefits:

1- Better fault tolerance. Amazon EC2 Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it. Also, Amazon EC2 Auto Scaling enables you to take advantage of the safety and reliability of geographic redundancy by spanning Auto Scaling groups across multiple Availability Zones within a Region. When one Availability Zone becomes unhealthy or unavailable, Auto Scaling launches new instances in an unaffected Availability Zone. When the unhealthy Availability Zone returns to a healthy state, Auto Scaling automatically redistributes the application instances evenly across all of the designated Availability Zones.

2- Better availability. Amazon EC2 Auto Scaling helps ensure that your application always has the right amount of capacity to handle the current traffic demand.

3- Better cost management. Amazon EC2 Auto Scaling can dynamically increase and decrease capacity as needed. Because you pay for the EC2 instances you use, you

save money by launching instances when they are needed and terminating them when they aren't.

The other options are incorrect:

"Auto Scaling Groups distributes application traffic across multiple Availability Zones to enhance performance" is incorrect. AWS ELB is the service that is used to distribute traffic. Auto Scaling Groups do not distribute traffic

"Auto Scaling Groups scales EC2 instances across multiple regions to reduce latency for global users" is incorrect. An Auto Scaling group can contain EC2 instances in one or more Availability Zones within the same Region. However, Auto Scaling groups cannot span multiple Regions.

"Auto Scaling Groups caches the most recent responses at global edge locations to reduce latency and improve performance" is incorrect. Amazon CloudFront is the service that is used to cache the most recent responses at global edge locations to provide faster performance for global users. Auto Scaling Groups do not perform any caching.

References:

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

Question 26:

Skipped

You have just hired a skilled sys-admin to join your team. As usual, you have created a new IAM user for him to interact with AWS services. On his first day, you ask him to create snapshots of all existing Amazon EBS volumes and save them in a new Amazon S3 bucket. However, the new member reports back that he is unable to create neither EBS snapshots nor S3 buckets. What might prevent him from doing this simple task?

-

The systems administrator must contact AWS Support first to activate his new IAM account

-
-

There is not enough space in S3 to store the snapshots

-
-

There is a non-explicit deny to all new users

(Correct)

-
-

EBS and S3 are accessible only to the root account owner

Explanation

When a new IAM user is created, that user has NO access to any AWS service. This is called a non-explicit deny. For that user, access must be explicitly allowed via IAM permissions.

The other options are incorrect:

"EBS and S3 are accessible only to the root account owner" is incorrect. EBS and S3 are accessible to any IAM User, Group, or Role with an attached policy that grants those permissions.

"The systems administrator must contact AWS Support first to activate his new IAM account" is incorrect. Account activation is not required for new IAM users. Account activation is required only for the AWS root account owner, and usually, this process is done automatically without contacting AWS Support.

"There is not enough space in S3 to store the snapshots" is incorrect. Amazon S3 provides virtually unlimited storage capacity.

References:

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

Question 27:

Skipped

A company's AWS workflow requires that it periodically perform large-scale image and video processing jobs. The customer is seeking to minimize cost and has stated that the amount of time it takes to process these jobs is not critical, but that cost minimization is the most important factor in designing the solution. Which EC2 instance class is best suited for this processing?

-
- EC2 Reserved Instances - All Upfront
-
- EC2 Spot Instances

(Correct)

-
- EC2 Reserved Instances - No Upfront
-
- EC2 On-Demand Instances

Explanation

A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable customers to request unused EC2 instances at steep discounts, customers can lower their Amazon EC2 costs significantly. Spot Instances run whenever capacity is available, and the maximum price per hour for the request exceeds the Spot price. The risk with Spot instances is that a running instance can be interrupted due to changes in demand and pricing for a specific class of Spot instances, as there is no guarantee of availability at any time. Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks, as well as for workloads that are not time critical.

The other options are incorrect:

"EC2 On-Demand Instances" is incorrect. The Spot option provides discounts up to 90% off compared to the On-Demand price, making this option less cost effective than the Spot Instance option.

"EC2 Reserved Instances - All Upfront" and "EC2 Reserved Instances - No Upfront" are incorrect. Use of reservations means that the customer will be charged the agreed upon Reserved Instance hourly rate irrespective of if the instance is running or not. Because these jobs are both periodic and non-time sensitive, Spot Instances are better suited for the task, and they offer a lower price point than Reserved Instances.

References:

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

Question 28:

Skipped

An AWS customer has used one Amazon Linux instance for 2 hours, 5 minutes and 9 seconds, and one CentOS instance for 4 hours, 23 minutes and 7 seconds. How much time will the customer be billed for?

- 3 hours for the Linux instance and 5 hours for the CentOS instance
 - 2 hours, 5 minutes and 9 seconds for the Linux instance and 4 hours, 23 minutes and 7 seconds for the CentOS instance
 - 2 hours, 5 minutes and 9 seconds for the Linux instance and 5 hours for the CentOS instance
- (Correct)**
- 3 hours for the Linux instance and 4 hours, 23 minutes and 7 seconds for the CentOS instance

Explanation

Amazon EC2 supports a variety of operating systems including: Amazon Linux, Ubuntu, Windows Server, CentOS, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, openSUSE Leap, Fedora, Fedora CoreOS, Debian, Gentoo Linux, Oracle Linux, and FreeBSD.

Per-second billing is available only for instances launched in Amazon Linux, Windows or Ubuntu.

With per-second billing in EC2 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.

For other instances, including CentOS, each partial instance-hour consumed will be billed as a full hour.

In this case, the customer will be charged for 2 hours, 5 minutes and 9 seconds for the Amazon Linux instance, and 5 hours for the CentOS instance.

References:

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

<https://aws.amazon.com/mp/linux/>

Question 29:

Skipped

What features does AWS offer to help protect your data in the Cloud? (Choose TWO)

- Unlimited storage
- Physical MFA devices
- Access control

(Correct)

-

Load balancing

-

Data encryption

(Correct)

Explanation

AWS offers a lot of services and features that help you protect your data in the cloud. You can protect your data by encrypting it in transit and at rest. You can use CloudTrail to log API and user activity, including who, what, and from where calls were made. You can also use AWS Identity and Access Management (IAM) to control who can access or change your data. You can also use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.

The customer is responsible for protecting their data in the following ways:

- 1- Data encryption (at rest and in transit)
- 2- Setting up access control
- 3- Monitoring user activity
- 4- Applying MFA
- 5- Using advanced managed security services such as Amazon Macie.

Additional information:

Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks. Today, Amazon Macie is available to protect data stored in Amazon S3, with support for additional AWS data stores coming later this year.

The other options are incorrect:

"Load balancing" is incorrect. There is no relation between Load Balancing and data protection. Load Balancing is the process of distributing incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.

"Physical MFA devices" is incorrect. MFA can help protect your data, but AWS does not provide physical MFA devices.

"Unlimited storage" is incorrect. AWS offers virtually unlimited storage for its customers, but this has nothing to do with data protection.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/data-protection.html>

<https://aws.amazon.com/iam/features/mfa/>

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

Question 30:

Skipped

Which of the following can be used to enable the Virtual Multi-Factor Authentication? (Choose TWO)

-

Amazon SNS

-

Amazon Connect

-

Amazon Virtual Private Cloud

-

AWS CLI

(Correct)

-

AWS Identity and Access Management (IAM)

(Correct)

Explanation

You can use either the AWS IAM console or the AWS CLI to enable a virtual MFA device for an IAM user in your account.

The other options are incorrect:

"Amazon SNS" is incorrect. Amazon Simple Notification Service (Amazon SNS) is a messaging service that makes it easy to set up, operate, and send notifications from AWS.

"Amazon Virtual Private Cloud" is incorrect. Amazon Virtual Private Cloud (Amazon VPC) allows you to define a virtual network in AWS.

"Amazon Connect" is incorrect. Amazon Connect is a cloud-based contact center service.

References:

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

Question 31:

Skipped

You are running a financial services web application on AWS. The application uses a MySQL database to store the data. Which of the following AWS services would improve the performance of your application by allowing you to retrieve information from fast in-memory caches?

-
- Amazon Neptune
-
- Amazon EFS
-
- Amazon ElastiCache

(Correct)

-

DAX

Explanation

Amazon ElastiCache offers fully managed Redis and Memcached. Seamlessly deploy, operate, and scale popular open source compatible in-memory data stores. Build data-intensive apps or improve the performance of your existing apps by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for Gaming, Ad-Tech, Financial Services, Healthcare, and IoT apps.

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:

"Amazon Neptune" is incorrect. Amazon Neptune is a graph database service.

"DAX" is incorrect. DAX is a caching feature for use with Amazon DynamoDB - which is a NoSQL database - and the application specified uses a MySQL database.

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

References:

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

Question 32:

Skipped

Which methods can be used by customers to interact with AWS Identity and Access Management (IAM)? (Choose TWO)

-

AWS Security Groups

-

AWS Network Access Control Lists

-

AWS SDKs

(Correct)

-

AWS CLI

(Correct)

-

AWS CodeCommit

Explanation

Customers can work with AWS Identity and Access Management in any of the following ways:

1- AWS Management Console: The console is a browser-based interface that can be used to manage IAM and AWS resources.

2- AWS Command Line Tools: Customers can use the AWS command line tools to issue commands at your system's command line to perform IAM and AWS tasks. Using the command line can be faster and more convenient than the console. The command line tools are also useful if you want to build scripts that perform AWS tasks. AWS provides two sets of command line tools: the AWS Command Line Interface (AWS CLI) and the AWS Tools for Windows PowerShell.

3- AWS SDKs: AWS provides SDKs (software development kits) that consist of libraries and sample code for various programming languages and platforms (Java, Python, Ruby, .NET, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to IAM and AWS. For example, the SDKs take care of tasks such as cryptographically signing requests, managing errors, and retrying requests automatically.

The other options are incorrect:

"AWS Security Groups" is incorrect. You can use security groups to control the inbound and outbound traffic for your instances.

"AWS Network Access Control Lists" is incorrect. Network Access Control Lists (NACLs) are used to provide fine-grained control of network traffic into and out of a subnet.

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

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html#intro-accessing>

Question 33:

Skipped

Which of the following approaches will help you eliminate human error and automate the process of creating and updating your AWS environment?

- Use AWS CodeDeploy to build and automate your AWS environment
- Migrate all of your applications to a dedicated host
- Use code to provision and operate your AWS infrastructure

(Correct)

- Use Software test automation tools

Explanation

In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events. By performing operations as code, you limit human error and enable consistent responses to events.

You can define your infrastructure as code using approaches such as AWS CloudFormation templates. The use of templates allows you to build and rebuild your infrastructure, without having to perform manual actions or write custom scripts.

Codifying your infrastructure in a template allows you to treat your infrastructure as just code. You can author it with any code editor, check it into a version control system, and review the files with team members before deploying into production. This gives developers an easy way to build and update their entire AWS environment in a timely fashion.

The other options are incorrect.

"Use AWS CodeDeploy to build and automate your AWS environment" is incorrect. AWS CodeDeploy cannot be used to manage the AWS infrastructure. AWS CodeDeploy is a service that automates application code deployments to Amazon EC2 instances and instances running on-premises.

"Use Software test automation tools" is incorrect. Software test automation tools enable you to simplify testing and reduce time to release by automating functional tests for your applications.

"Migrate all of your applications to a dedicated host" is incorrect. Dedicated Hosts provide you with EC2 instance capacity on physical servers dedicated to your use. You may need to migrate your applications to a dedicated host to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2 so that you get the flexibility and cost-effectiveness of using your own licenses, but with the resiliency, simplicity, and elasticity of AWS. Amazon EC2 Dedicated Hosts can also help address corporate compliance requirements because they are dedicated only to a single customer.

References:

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

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

Question 34:

Skipped

Which AWS Service helps enterprises extend their on-premises storage to AWS in a cost-effective manner?



AWS Storage Gateway

(Correct)

- Amazon Aurora
- Amazon EFS
- AWS Data Pipeline

Explanation

Enterprises can extend their on-premises storage to AWS Cloud for long-term backup retention and archiving, optimizing costs and increasing resilience and availability. AWS Storage Gateway is a hybrid storage service that enables on-premises applications to seamlessly use AWS cloud storage. Enterprises can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration. The storage gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS, and AWS Backup, providing storage for files, volumes, snapshots, and virtual tapes in AWS.

The other options are incorrect:

Amazon Aurora is incorrect. Amazon Aurora is a MySQL and PostgreSQL-compatible relational database service.

Amazon EFS is incorrect. Amazon Elastic File System (Amazon EFS) provides fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Although EFS can be used in hybrid environments, it is not as cost-effective as Storage Gateway.

AWS Data Pipeline is incorrect. AWS Data Pipeline is a web service that helps customers reliably process and move data between different AWS compute and

storage services, as well as on-premises data sources. AWS Data Pipeline is not a storage service.

References:

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

Question 35:

Skipped

Which of the following are examples of the customer's responsibility to implement "security **IN** the cloud"? (Choose TWO)

- Creating a new hypervisor
- Building a schema for an application

(Correct)

- Replacing physical hardware
- Patch management of the underlying infrastructure
- File system encryption

(Correct)

Explanation

"Security **IN** the Cloud" refers to the Customer's responsibility in the Shared Responsibility Model. Customers are responsible for items such as building application schema, monitoring server and application performance, configuring security groups and network ACLs, and encrypting their data.

"Security **OF** the Cloud" refers to the AWS' responsibility in the Shared Responsibility Model. AWS is responsible for items such as the physical security of the DC (data center), creating hypervisors, replacement of old disk drives, and patch management of the infrastructure.

NOTE:

For "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.

References:

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

Question 36:

Skipped

You decide to buy a reserved instance for a term of one year. Which option provides the largest total discount?

-
-

Partial up-front reservation

-
-

All reserved instance payment options provide the same discount level

-
-

No up-front reservation

-
-

All up-front reservation

(Correct)

Explanation

There are three payment options available when purchasing reserved instances:

1- No up-front

2- Partial up-front

3- All up-front.

The general rule is: "the more you spend upfront, the more discounts you get."

With the All Upfront option, you pay for the entire Reserved Instance term with one upfront payment. This option provides you with the largest discount compared to On-Demand instance pricing.

The other options are incorrect:

"No up-front reservation" is incorrect. The No up-front option does not require any upfront payment and provides a discounted hourly rate for the duration of the term. But the price will be higher compared to other options because there was no up-front payment.

"Partial up-front reservation" is incorrect. With the Partial Upfront option, you make a low upfront payment and are then charged a discounted hourly rate for the instance for the duration of the Reserved Instance term. The price of the instance will be more than the price of the instance purchased using the "All up-front option" because, with the Partial up-front option, you pay less up-front. Hence, the correct answer is All up-front.

References:

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

Question 37:

Skipped

Which features are included in the AWS Business Support Plan? (Choose TWO)

-

Partial access to the core Trusted Advisor checks

-

24x7 access to customer service

(Correct)

- Access to the Infrastructure Event Management (IEM) feature for additional fee

(Correct)

- 24x7 access to the TAM feature
-

Access to Cloud Support Engineers via email only during business hours

Explanation

All AWS support plans (including the Business plan) provide 24x7 access to AWS Customer Service.

The Business support plan provides access to Infrastructure Event Management for additional fee. AWS Infrastructure Event Management is a structured program available to Enterprise Support customers (and Business Support customers for an additional fee) that helps customers plan for large-scale events such as product or application launches, infrastructure migrations, and marketing events.

The other options are incorrect:

"24x7 access to the TAM feature" is incorrect. The Enterprise support plan is the only plan that provides access to the Technical Account Manager (TAM) feature

"Access to Cloud Support Engineers via email only during business hours" is incorrect. The Business support plan provides 24x7 access to Cloud Support Engineers via phone, email, and chat.

"Partial access to the core Trusted Advisor checks" is incorrect. AWS Business Support Plans and Enterprise Support Plans both provide full set of Trusted Advisor checks.

AWS **Basic** Support and AWS **Developer** Support customers get access to 6 security checks (S3 Bucket Permissions, Security Groups - Specific Ports Unrestricted, IAM Use, MFA on Root Account, EBS Public Snapshots, RDS Public Snapshots) and 50 service limit checks.

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

References:

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

Question 38:

Skipped

Which AWS Service can perform health checks on Amazon EC2 instances?



Amazon Route 53

(Correct)



Amazon Aurora



AWS CloudFormation



Amazon Chime

Explanation

Amazon Route 53 provides highly available and scalable Domain Name System (DNS), 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 offers health checks to monitor the health and performance of your application as well as your web servers and other resources. Route 53 can be configured to route traffic only to the healthy endpoints to achieve greater levels of fault tolerance in your applications.

Note: The Elastic Load Balancing service also performs health checks on Amazon EC2 instances and distribute traffic only to the healthy ones.

The other options are incorrect:

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

Amazon Chime is incorrect. Amazon Chime is a communications service for online meetings.

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

References:

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

Question 39:

Skipped

A company is developing a mobile application and wants to allow users to use their Amazon, Apple, Facebook, or Google identities to authenticate to the application. Which AWS Service should the company use for this purpose?

-

Amazon GuardDuty

-
- Amazon Cognito
- (Correct)**
-
- Amazon Personalize
-
- AWS IAM

Explanation

Amazon Cognito lets customers add user sign-up, sign-in, and access control to their web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0.

The other options are incorrect:

"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 groups, and use permissions to allow and deny their access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to access and use AWS resources. **AWS IAM is an authentication \ authorization service like Amazon Cognito**, but it does not provide user sign-up, sign-in, and access control to web and mobile applications.

"Amazon Personalize" is incorrect. Amazon Personalize is a fully managed machine learning service that can be used to **deliver highly customized recommendations** to customers across industries such as retail, media and entertainment. Amazon Personalize enables developers to build applications with the same machine learning (ML) technology used by Amazon.com for real-time personalized recommendations. Amazon Personalize can be used to personalize the end-user experience over any digital channel. Examples include product recommendations for e-commerce, news articles and content recommendation for publishing, media and social networks, hotel recommendations for travel websites, and credit card recommendations for banks.

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

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

References:

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

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

Question 40:

Skipped

Which AWS Service allows customers to download AWS SOC & PCI reports?

-
-

AWS Well-Architected Tool

-
-

AWS Artifact

(Correct)

-
-

AWS Glue

-
-

Amazon Chime

Explanation

AWS Artifact provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports. You can submit the security and compliance documents (also known as audit artifacts) to your auditors or regulators to demonstrate the security and compliance of the AWS infrastructure and services that you use. You can also use these documents as guidelines to evaluate your own cloud architecture and assess the effectiveness of your company's internal controls.

The other options are incorrect:

"Amazon Chime" is incorrect. Amazon Chime is an AWS communications service that is used for online meetings, video conferencing, calls, and chat.

"AWS Well-Architected Tool" is incorrect. The AWS Well-Architected Tool helps customers review the state of their workloads and compares them to the latest AWS architectural best practices. The tool is based on the [AWS Well-Architected Framework](#), developed to help cloud architects build secure, high-performing, resilient, and efficient application infrastructure.

"AWS Glue" is incorrect. AWS Glue is a fully-managed, pay-as-you-go, extract, transform, and load (ETL) service that automates the time-consuming steps of data preparation for analytics.

References:

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

Question 41:

Skipped

Which of the following should be taken into account when performing a TCO analysis regarding the costs of running an application on AWS VS on-premises? (Choose TWO)

-

Software architecture

- Amazon EBS computing power
- Labor and IT costs

(Correct)

- Software compatibility
- Cooling and power consumption

(Correct)

Explanation

Weighing the financial considerations of owning and operating a data center facility versus employing a cloud infrastructure requires detailed and careful analysis. In practice, it is not as simple as just measuring potential hardware expense alongside utility pricing for compute and storage resources. The Total Cost of Ownership (TCO) is often the financial metric used to estimate and compare direct and indirect costs of a product or a service. Cooling and power consumption, data center space, data center real estate and Labor IT cost are examples of the indirect costs of a physical data center and should be included in TCO analysis.

Additional information:

Labor IT costs include the cost of the sizable IT infrastructure teams that are needed to handle the "heavy lifting" of managing physical infrastructure:

1- Hardware procurement teams are needed. These teams have to spend a lot of time evaluating hardware, negotiating contracts, holding hardware vendor meetings, managing delivery and installation, etc. It's expensive to have a staff with sufficient knowledge to do this well.

2- Data center design and build teams are needed to create and maintain reliable and cost-effective facilities. These teams need to stay up-to-date on data center

design and be experts in managing heterogeneous hardware and the related supply chain, managing legacy software, moving facilities, scaling and managing physical growth—all the tasks that an enterprise needs to do well if it wants to achieve low incremental costs.

3- Operations staff is needed 24/7/365 in each facility.

4- Database administration teams are needed to manage the databases. This staff is responsible for installing, patching, upgrades, migration, backups, snapshots and recovery of databases, ensuring availability, troubleshooting, and performance enhancements.

5- Networking teams are needed for running a highly available network. Expertise is needed to design, debug, scale, and operate the network and deal with the external relationships necessary to have cost-effective Internet transit.

6- Security personnel are needed at all phases of the design, build, and operations process.

The other options are incorrect.

"Software compatibility" and "Software architecture" are incorrect. In the scenario, the Total Cost of Ownership (TCO) is the total cost of owning and operating a data center, including facilities, physical servers, storage devices, networking equipment, cooling and power consumption, data center space, Labor, and IT costs. "Software compatibility" and "software architecture" are not part of the total cost of owning and operating a data center (TCO), and thus are incorrect answers.

"Amazon EBS computing power" is incorrect. Amazon EBS is a block storage service that creates volumes to be used by EC2 instances.

References:

<https://aws.amazon.com/blogs/publicsector/cloud-economics-value-tco-assessment/>

Question 42:

Skipped

Which of the following is true regarding the AWS availability zones and edge locations?

-

An availability zone exists within an edge location to distribute content globally with low latency

-

An AWS Availability Zone is an isolated location within an AWS Region, however edge locations are located in multiple cities worldwide

(Correct)

-

Edge locations are located in separate Availability Zones worldwide to serve global customers

-

An Availability Zone is a geographic location where AWS provides multiple, physically separated and isolated edge locations

Explanation

In AWS, each Region has multiple, isolated locations known as Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

Edge locations may or may not exist within a region. They are located in most major cities around the world. Edge locations are specifically used by CloudFront (CDN) to distribute content to global users with low latency.

The other options are incorrect:

"An availability zone exists within an edge location to distribute content globally with low latency" is incorrect. An availability zone exists within an AWS Region, not within an edge location

"Edge locations are located in separate Availability Zones worldwide to serve global customers" is incorrect. Edge locations are located in most major cities around the world. Edge locations may or may not exist within a given AWS Region.

"An Availability Zone is a geographic location where AWS provides multiple, physically separated and isolated edge locations" is incorrect. An availability zone exists within an AWS Region. Edge locations are located in most major cities around the world. Edge locations may or may not exist within a given AWS Region.

References:

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

Question 43:

Skipped

Which of the following services can be used to monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront?

- AWS WAF
- (Correct) Amazon CloudWatch
- AWS CloudTrail
- AWS Cloud9

Explanation

AWS WAF is a web application firewall that lets customers monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an Application Load Balancer. AWS WAF also lets customers control access to their content by defining customizable web security rules.

The other options are incorrect:

AWS CloudTrail is incorrect. AWS CloudTrail is a logging service that tracks and records user activity and API usage for audit purposes.

Amazon CloudWatch is incorrect. Amazon CloudWatch is used to monitor the utilization of the AWS cloud resources (such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances), as well as custom metrics generated by applications and services.

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

References:

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

Question 44:

Skipped

A company is seeking to deploy an existing .NET application onto AWS as quickly as possible. Which AWS Service should the customer use to achieve this goal?

-
-

AWS Amplify

-
-

AWS Systems Manager

-
-

AWS Trusted Advisor



AWS Elastic Beanstalk

(Correct)

Explanation

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

The other options are incorrect:

"AWS Amplify" is incorrect. AWS Amplify is used for **building** secure and scalable web and mobile applications, not **deploying** applications.

"AWS Trusted Advisor" is incorrect. AWS Trusted Advisor analyzes AWS environments and provides best practice recommendations in five categories: cost optimization, security, fault tolerance, performance and service limits.

"AWS Systems Manager" is incorrect. AWS Systems Manager allows customers to centralize operational data from multiple AWS services and automate tasks across their AWS resources.

References:

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

Question 45:

Skipped

Which AWS Service allows customers to create a template that programmatically defines policies and configurations of all AWS resources as code and so that the same template can be reused among multiple projects?

-
- AWS Config
-
- AWS Auto Scaling
-
- AWS CloudTrail
-
- AWS CloudFormation

(Correct)

Explanation

AWS CloudFormation is a service that helps customers model and set up their Amazon Web Services resources so that they can spend less time managing those resources and more time focusing on their applications that run in AWS. Customers create a template that describes all the AWS resources that they want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning those resources for them.

Also, Customers can create an AWS CloudFormation script that captures their security policies, networking policies, and other aspects of configuration and reliably deploys it. Security best practices can then be reused among multiple projects and become part of a continuous integration pipeline.

The other options are incorrect:

AWS Auto Scaling is incorrect. AWS Auto Scaling is used to adjust capacity (up or down) automatically to optimize performance and costs.

AWS CloudTrail is incorrect. AWS CloudTrail is a logging service that tracks and records user activity and API usage for audit purposes.

AWS Config is incorrect. AWS Config is used to record and evaluate configurations of your AWS resources.

References:

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

Question 46:

Skipped

Which IAM entity can best be used to grant temporary access to your AWS resources?



IAM Groups



IAM Users



Key Pair



IAM Roles

(Correct)

Explanation

An IAM role is an IAM entity that defines a set of permissions for making AWS service requests. IAM roles are not associated with a specific user or group. Instead, trusted entities assume roles, such as IAM users, applications, or AWS services such as EC2. 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 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.

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 temporary access to AWS resources using an IAM role.

The other options are incorrect.

"IAM Users" is incorrect. An IAM user has permanent long-term credentials, not temporary credentials.

"IAM Groups" is incorrect. An IAM Group is a way to logically manage sets of IAM Users who require identical permissions.

"Key Pair" is incorrect. Amazon EC2 Key Pair enables you to securely access your instances using a private key instead of a password. You can create and download this Key Pair when launching a new EC2 instance.

Additional information:

Key Pair is different than the AWS Access Keys. Access Keys are security credentials (like a user name and password) that allow users to interact with AWS services programmatically.

References:

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

Question 47:

Skipped

What are the capabilities of AWS X-Ray? (Choose TWO)

- Automatically decouples application components
- Deploys applications to on-premises servers
- Helps improve application performance

(Correct)

- Facilitates tracking of user requests to identify application issues
- **(Correct)**
- Deploys applications to Amazon EC2 instances

Explanation

Benefits of AWS X-Ray include:

1- Review request behavior:

AWS X-Ray traces user requests as they travel through your entire application. It aggregates the data generated by the individual services and resources that make up your application, providing you an end-to-end view of how your application is performing.

2- Discover application issues:

With AWS X-Ray, you can glean insights into how your application is performing and discover root causes. With X-Ray's tracing features, you can follow request paths to pinpoint where in your application and what is causing performance issues.

3- Improve application performance

AWS X-Ray helps you identify performance bottlenecks. X-Ray's service maps let you see relationships between services and resources in your application in real time. You can easily detect where high latencies are occurring, visualize node and edge latency distribution for services, and then drill down into the specific services and paths impacting application performance.

The other options are incorrect.

"Deploys applications to Amazon EC2 instances" is incorrect. AWS X-Ray does not deploy applications. The AWS services that can help you deploy your applications to Amazon EC2 instances include: AWS Elastic Beanstalk, AWS CloudFormation, AWS CodeDeploy and AWS OpsWorks.

"Deploys applications to on-premises servers" is incorrect. AWS X-Ray does not deploy applications. The AWS services that can help you deploy your applications to on-premises servers include: AWS CodeDeploy and AWS OpsWorks.

Note: You cannot use AWS Elastic Beanstalk or AWS CloudFormation to deploy your applications to on-premises servers.

"Enables you to decouple your application components" is incorrect. AWS X-Ray does not automatically decouple application components, and no AWS Services automatically decouple application components. The AWS services that can help you decouple your applications include: Amazon Simple Queue Service (SQS) and Amazon Simple Notification Service (SNS).

References:

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

<https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-on-aws.pdf>

<https://aws.amazon.com/about-aws/whats-new/2014/12/08/aws-opsworks-supports-existing-ec2-instances-and-on-premises-servers/>

<https://aws.amazon.com/blogs/aws/aws-codedeploy-update-new-support-for-on-premises-instances/>

Question 48:

Skipped

A company has a web application that is hosted on a single EC2 instance and is approaching 100 percent CPU Utilization during peak loads. Rather than scaling the server vertically, the company has decided to deploy three Amazon EC2 instances in parallel and to distribute traffic across the three servers. What AWS Service should the company use to distribute the traffic evenly?

-

AWS Application Load Balancer (ALB)

(Correct)

-

Amazon CloudFront

-

AWS Global Accelerator

-

Transit VPC

Explanation

AWS Application Load Balancer (ALB) is part of the AWS Elastic Load Balancing family that is specifically designed to handle HTTP and HTTPS traffic. An ALB automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. Once you register the Amazon EC2 instances with the ALB, it automatically distributes the incoming traffic across those instances. The Load Balancer also performs health checks on the instances and routes traffic only to the healthy ones.

The other options are incorrect:

"Amazon CloudFront" is incorrect. Amazon CloudFront is the AWS' Content Distribution Network (CDN) and is used to distribute content to global users with low latency.

"Transit VPC" is incorrect. A transit Virtual Private Cloud (VPC) is a common strategy for connecting multiple, geographically disperse VPCs and remote networks in order to create a global network transit center. Transit VPCs help organizations transfer data from one Amazon VPC to another, simplifying operations and eliminating the latency issues by peering between resources.

"AWS Global Accelerator" is incorrect. AWS Global Accelerator uses the AWS global network to improve the availability and performance of the applications that you offer to your global users. AWS Global Accelerator does not perform load balancing functions.

References:

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

Question 49:

Skipped

A user has opened a "Production System Down" support case to get help from AWS Support after a production system disruption. What is the expected response time for this type of support case?

- 15 minutes
 - 24 hours
 - One hour
- (Correct)**
- 12 hours

Explanation

Customers with AWS Business or Enterprise support plans can open a "Production System Down" support case. The response time for this type of support case is one hour.

Similarly, the response time for the "Business-critical system down" support case is 15 minutes. But, AWS customers must have an Enterprise support plan to be able to open this support case.

References:

<https://docs.aws.amazon.com/awssupport/latest/user/case-management.html>

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

Question 50:

Skipped

When granting permissions to applications running on Amazon EC2 instances, which of the following is considered best practice?

-
-

Store the required AWS credentials directly within the application code

-
-

Do nothing; Applications that run on Amazon EC2 instances do not need permission to interact with other AWS services or resources

-
-

Generate new IAM access keys every time you delegate permissions

-
-

Use temporary security credentials (IAM roles) instead of long-term access keys

(Correct)

Explanation

AWS recommends using an IAM role to manage temporary credentials for applications that run on Amazon EC2 instances. When you use a role, you don't have to distribute long-term credentials (such as a user name and password or access

keys) to an EC2 instance. Instead, the role supplies temporary permissions that applications can use when they interact with other AWS resources. For example, if you have a photo-editing application running on an Amazon EC2 instance, and you want to grant the application permission to save user's photo uploads to an Amazon S3 bucket, it is best to use an IAM role to delegate the required permissions because role credentials are temporary and rotated automatically.

IAM roles with temporary credentials are useful in the following situations:

Applications running on Amazon EC2: You can use an IAM role to manage temporary credentials for applications running on an EC2 instance and make AWS CLI or AWS API requests. This is more secure than storing access keys within the EC2 instance.

Federated user access: Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an identity provider.

AWS service access: A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM.

The other options are incorrect:

"Store the required AWS credentials directly within the application code" is incorrect. It is not secure to store AWS credentials (such as a username and password or access keys) within the application code. Storing credentials directly in application code often results in long-lived credentials being saved in source control, which increases the attack surface of your application.

"Do nothing; Applications that run on Amazon EC2 instances do not need permission to interact with other AWS services or resources" is incorrect. Amazon EC2 and all other AWS services start with no permissions. Applications running on Amazon EC2 or any other compute service cannot interact with other AWS resources without permission.

"Generate new IAM access keys every time you delegate permissions" is incorrect. It is not secure to use long-term credentials (such as a username and password or access keys) to delegate permissions to applications running on Amazon EC2 instances. Using IAM roles is more secure because role credentials are temporary and rotated automatically.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

Question 51:

Skipped

One of the major advantages of using AWS is cost savings. What does AWS provide to reduce the cost of running Amazon EC2 instances?

- Low instance start-up fees
- Low-cost instance tagging
- Per-second instance billing

(Correct)

- Low monthly instance maintenance costs

Explanation

With per-second billing, customers pay for only what they use. It takes the cost of unused minutes and seconds in an hour off of the bill, so they can focus on improving their applications instead of maximizing usage to the hour. Especially, if a customer manages instances running for irregular periods of time, such as dev/testing, data processing, analytics, batch processing, and gaming applications, can benefit.

Usage of Amazon EC2 Linux, Windows, or Ubuntu instances is billed in one-second increments, with a minimum of 60 seconds. Similarly, provisioned storage for EBS volumes will be billed per-second increments, with a 60-second minimum. Per-second billing also applies to several other AWS services, including Amazon RDS, Amazon EMR, and AWS Batch.

The other options are incorrect:

"Low-cost instance tagging" is incorrect. There is no charge for tagging EC2 instances; it is a free feature.

"Low instance start-up fees" is incorrect. There are no instance start-up fees when using EC2.

"Low monthly instance maintenance costs" is incorrect. There are no additional maintenance costs for running an EC2 instance; the only cost for running an EC2 instance is the associated hourly cost.

References:

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

Question 52:

Skipped

Which AWS Group assists customers in achieving their desired business outcomes?

-

AWS Trusted Advisor

-

AWS Professional Services

(Correct)

AWS Concierge Support Team

AWS Security Team

Explanation

Moving to AWS provides customers with sustainable business advantages. Choosing to supplement teams with specialized skills and experience can help customers achieve those results. The AWS Professional Services organization is a global team of experts that helps customers realize their desired business outcomes when using AWS.

The other options are incorrect:

AWS Concierge Support Team is incorrect. The Concierge Team are AWS billing and account experts that work with you to implement billing and account best practices.

AWS Trusted Advisor is incorrect. AWS Trusted Advisor is not a team, it is an online tool that 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 Security Team is incorrect. The AWS Security Team is responsible for the security of services offered by AWS.

References:

<https://aws.amazon.com/professional-services/>

Question 53:

Skipped

A company is planning to use Amazon S3 and Amazon CloudFront to distribute its video courses globally. What tool can the company use to estimate the costs of these services?

-
- AWS Budgets
-
- AWS Pricing Calculator
(Correct)
-
- AWS Cost & Usage Report
-
- AWS Cost Explorer

Explanation

The AWS Pricing Calculator helps you estimate your monthly AWS bill more efficiently. The calculator can be used to determine your best and worst case scenarios and identify areas of development to reduce your monthly costs. The AWS Pricing Calculator is continuously updated with the latest pricing for all AWS services in all Regions. The AWS Pricing Calculator is available at: <https://calculator.aws/>

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. You can also set up AWS Budgets to alert you when your reservation utilization drops below the threshold you define.

"AWS Cost & Usage Report" is incorrect. The AWS Cost & Usage Report does not estimate costs. The AWS Cost & Usage Report enables customers to access detailed information related to their AWS costs and usage. This information can help them analyze their cost drivers and usage trends.

"AWS Cost Explorer" is incorrect.

AWS Cost Explorer is used to explore and analyze your historical spend and usage. AWS Cost Explorer allows you to have visibility into your consumption patterns, such as, mapping the most commonly used services, and identifying unexpected anomalies or expenses.

AWS Cost Explorer can also be used to estimate AWS services costs, but it calculates these estimates based on your previous AWS consumption (meaning AWS Cost Explorer is suitable for **existing projects only**). In the above scenario, AWS Pricing Calculator is the right choice because it can be used to estimate the costs of **both existing and new projects** (in our case, it is a new project).

AWS Pricing Calculator enables you to estimate the monthly cost of AWS services for your use case based on your expected usage (not based on previous consumption as is the case with AWS Cost Explorer). For example, if you expect to use 500 GB of S3 Standard storage, you can simply enter this value in the appropriate field and the calculator provides an estimate of your monthly bill.

Additional information:

AWS Cost Explorer Forecasting provides an estimate of what your AWS bill will be, based on your past usage. AWS Cost Explorer segments your historical data based on distinct charge types (e.g., on-demand usage, reserved instance usage, and more) and uses a combination of machine learning and rules-based models to predict spend across all of those charge types individually.

References:

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

<https://calculator.aws/>

Question 54:

Skipped

According to best practices, which of the below options is best suited for processing a large number of binary files?

- Vertically scaling RDS instances
- Running RDS instances in parallel
- Running EC2 instances in parallel
(Correct)
- Vertically scaling EC2 instances

Explanation

One of the core principles of the AWS Well-Architected Framework is that of scaling horizontally. Horizontal scaling means adding several smaller instances when workloads increase, instead of adding additional CPU, memory, or disk capacity to a single instance. In the syntax of this question, running several EC2 instances in parallel achieves horizontal scalability and is the correct answer.

AWS recommends that customers should scale resources horizontally to increase aggregate system availability. Replacing a large resource with multiple small resources in parallel will reduce the impact of a single failure on the overall system. For example, if a customer wants to convert a large number of binary files to text files or transcode a large number of video files to another format, it is recommended that they use multiple EC2 instances in parallel instead of using one large instance.

The other options are incorrect:

"Vertically scaling EC2 instances" is incorrect. Horizontal scaling is recommended over vertical scaling.

"Vertically scaling RDS instances" and "Running RDS instances in parallel" are incorrect. RDS instances are used to store and run databases and would not be used for file processing.

References:

<https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/>

Question 55:

Skipped

A company is migrating a web application to AWS. The application's compute capacity is continually utilized throughout the year. Which of the below options offer the company the most cost-effective solution? (Choose TWO)

- Dedicated Hosts
- Savings Plans
- On-demand Instances
- Reserved Instances

(Correct)

- Spot Instances

Explanation

For Customers that can commit to using EC2 over a 1 or 3-year term, it is better to use Amazon EC2 Reserved Instances or AWS Savings Plans. Reserved Instances and AWS Savings Plans provide a significant discount (up to 72%) compared to On-Demand instance pricing.

Reserved Instances:

Amazon EC2 Reserved Instances provide a significant discount compared to On-Demand pricing for customers that can commit to using EC2 over a 1- or 3-year term to reduce their total computing costs. Depending on the term of commitment and the amount paid up-front, discounts as high as 72% can be attained vs. On-Demand pricing.

Savings Plans:

Savings Plans offer significant savings over On Demand, just like EC2 Reserved Instances, in exchange for a commitment to use a specific amount of compute power (measured in \$/hour) for a one or three year period.

The difference between AWS Savings Plans and Reserved Instances is that Savings Plans provides you with the flexibility to use the instance configurations that best meet your needs, instead of making a commitment to a specific instance configuration (as is the case with reserved instances). For example, with Compute Savings Plans, if you commit to \$10 of compute usage an hour, you can use as many instances as you need (of any type) and you will get the Savings Plans prices on that usage up to \$10 and any usage beyond the commitment will be charged On Demand rates.

The other options are incorrect:

"On-demand Instances" is incorrect. With On-Demand instances, customers pay for compute capacity by the hour or the second depending on which instances they run. No longer-term commitments or upfront payments are needed. They can increase or decrease the compute capacity depending on the demands of their application and only pay for what they use. On-demand is recommended for customers who need consistent performance for a short period of time. On-demand instances are significantly less cost-effective than reserved instances.

"Spot Instances" is incorrect. Spot instances allow customers to take advantage of excess AWS EC2 capacity by paying a lower hourly price than the On-Demand price. Spot instances are not well suited for production workloads by themselves because the instance can be interrupted at any time if capacity is no longer available. Use cases of Spot instances include batch processing tasks and background jobs.

"Dedicated Hosts" is incorrect. Amazon EC2 Dedicated Hosts are used to help meet corporate compliance requirements and save money on licensing costs by enabling customers to use their existing software licenses from vendors such as Microsoft and Oracle on Amazon EC2.

References:

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

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

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

Question 56:

Skipped

Which of the below options is a best practice for making your application on AWS highly available?

-
-

Deploy the application to at least two Availability Zones

(Correct)

-
-

Rewrite the application code to handle all incoming requests

-
-

Deploy the application code on at least two servers in the same Availability Zone

-
-

Use Elastic Load Balancing (ELB) across multiple AWS Regions

Explanation

Each AWS Region contains multiple distinct locations, or Availability Zones. Each Availability Zone is engineered to be independent from failures in other Availability Zones. Deploying your application to multiple Availability Zones will increase the availability of your application. If one availability zone encounters an issue, the other availability zones can still serve your application.

The other options are incorrect:

"Use Elastic Load Balancing (ELB) across multiple AWS Regions" is incorrect. Elastic Load Balancing (ELB) is a regional service, not a global service. Elastic Load Balancing can only be used to distribute traffic across multiple Availability Zones within the same AWS Region.

"Deploy the application code on at least two servers in the same Availability Zone" is incorrect. Using more AWS servers in the same Availability Zone would help with performance so long as the Availability Zone had no issues, but being deployed to only one Availability Zone constitutes a single point of failure and is therefore not a best practice.

"Rewrite the application code to handle all incoming requests" is incorrect. There is no relation between the application code and "high availability". Even perfectly written code that never crashes will become unavailable if the infrastructure it runs on fails.

References:

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

Question 57:

Skipped

A company is building an online cloud storage platform. They need a storage service that can scale capacity automatically, while minimizing cost. Which AWS storage service should the company use to meet these requirements?

-
- AWS Storage Gateway
-
- Amazon Elastic Container Service
-

Amazon Simple Storage Service

(Correct)

-

Amazon Elastic Block Store

Explanation

Amazon S3 is a storage service offered by AWS that offers highly redundant object storage to AWS customers. Amazon S3 allows customers to effectively store and retrieve any amount of data from anywhere. Amazon S3 offers an extremely durable, highly available, and infinitely scalable data storage infrastructure at very low costs.

The other options are incorrect:

Amazon Elastic Container Service is incorrect. Amazon Elastic Container Service (Amazon ECS) is a container orchestration service that is used to run containerized applications on AWS.

Amazon Elastic Block Store is incorrect. Amazon Elastic Block Store is a block storage offering inside of AWS. While EBS can be configured to be highly performant, it is significantly more expensive than S3, and requires configuration modifications to grow the device capacity.

Amazon EBS can only be used as a drive for Amazon EC2 or Amazon RDS instances. Amazon EBS is designed for application workloads that benefit from fine tuning for performance and capacity. Typical use cases include Big Data analytics engines (like the Hadoop/HDFS ecosystem and Amazon EMR clusters), relational and NoSQL databases (like Microsoft SQL Server and MySQL or Cassandra and MongoDB), stream and log processing applications (like Kafka and Splunk), and data warehousing applications (like Vertica and Teradata).

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

References:

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

Question 58:

Skipped

Availability Zones within a Region are connected over low-latency links. Which of the following is a benefit of these links?

-
-

Automate the process of provisioning new compute resources

-
-

Achieve global high availability

-
-

Make synchronous replication of your data possible

(Correct)

-
-

Create private connection to your data center

Explanation

Each AWS Region contains multiple distinct locations, or Availability Zones. Each Availability Zone is engineered to be independent from failures in other Availability Zones. An Availability Zone is a data center, and in some cases, an Availability Zone consists of multiple data centers. Availability Zones within a Region provide inexpensive, low-latency network connectivity to other zones in the same Region. This allows you to replicate data across data centers in a synchronous manner so that failover can be automated and appear transparent to your users.

The other options are incorrect:

"Create private connection to your data center" is incorrect. The AWS Direct Connect service is the service that can be used to establish a private connection between AWS and your datacenter.

"Automate the process of provisioning new compute resources" is incorrect. There is no relation between low-latency links and provisioning new resources. Auto Scaling is the service that can be used to automate the process of creating new compute resources.

"Achieve global high availability" is incorrect. You cannot achieve global high availability by merely using Availability Zones within the same Region. You should deploy your application in multiple regions closest to your users or use the AWS CloudFront service to achieve high global availability.

References:

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

Question 59:

Skipped

A company is seeking to better secure its AWS account from unauthorized access. Which of the below options can the customer use to achieve this goal?

- Require Multi-Factor Authentication (MFA) for all IAM User access
- (Correct)**
- Set up two login passwords
- Restrict any API call made through SDKs or CLI
- Create one IAM account for each department in the company (Development, QA, Production), and share it across all staff in that department

Explanation

For increased security, AWS recommends that you configure multi-factor authentication (MFA) to help protect your AWS resources. MFA adds extra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services. You can also enforce MFA authentication for AWS service APIs via AWS Identity and Access Management (IAM) policies. This provides an extra layer of security over powerful API operations that you designate, such as terminating Amazon EC2 instances or reading sensitive data stored in Amazon S3.

The other options are incorrect:

"Restrict any API call made through SDKs or CLI" is incorrect. There is nothing wrong with using the AWS SDKs or CLI to interact with AWS services and resources. The API calls made through them can be secured using the AWS Access Keys and the AWS IAM permissions.

"Set up two login passwords" is incorrect. AWS doesn't allow this. Also, it may not improve security because it is the same mechanism.

"Create one IAM account for each department in the company (Development, QA, Production), and share it across all staff in that department" is incorrect. It is a best practice for each IAM User to have their own account. Sharing credentials makes it difficult, if not impossible, to audit which user performed specific actions.

Additional information:

To make programmatic requests to AWS services using SDKs you must provide valid credentials (Access key ID and secret access key) when setting up your SDK and must also have the IAM permissions that allow you to interact with these services.

AWS CLI is just like the AWS SDKs, you must provide valid credentials (Access key ID and secret access key) when configuring your CLI. To interact with AWS services using the AWS CLI, you must also have the required IAM permissions to use these services.

References:

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

Question 60:

Skipped

Your company requires a response time of less than 15 minutes from support interactions about their business-critical systems that are hosted on AWS if those systems go down. Which AWS Support Plan should this company use?



AWS Basic Support



AWS Developer Support



AWS Business Support



AWS Enterprise Support

(Correct)

Explanation

AWS support plans provide different response times based on the case's severity. For example, the Enterprise plan provides General Guidance within 24 hours. However, if the case involves a business-critical system being down, the company will get a response within 15 minutes.

The other options are incorrect.

Business is incorrect. The AWS Business Support Plan offers a 1-hour response time for a production system down, which does not meet the 15-minute criteria set forth in the question stem.

Developer is incorrect. The AWS Developer Support Plan offers a 12-hour response time for an impaired or down system, which does not meet the 15-minute criteria set forth in the question stem.

Basic is incorrect. Technical Support is not part of the Basic support plan.

References:

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

Question 61:

Skipped

Which of the following will help AWS customers save on costs when migrating their workloads to AWS?

- Use servers instead of managed services
 - Use existing third-party software licenses on AWS
- (Correct)**
- Migrate production workloads to AWS edge locations instead of AWS Regions
 - Use AWS Outposts to run all workloads in a cost-optimized environment

Explanation

AWS Customers who have already purchased software licenses - from vendors such as Microsoft and Oracle - can reuse these licenses on AWS instead of buying new licenses. For software that consumes licenses on a per-core or per-socket basis, such as Windows Server and SQL Server, AWS customers may need to migrate their workloads to a dedicated host to use this type of software license.

The other options are incorrect:

"Use servers instead of managed services" is incorrect. AWS recommends the use of managed services instead of servers where possible. AWS offers a broad set of compute, storage, database, analytics, application, and deployment services that help organizations move faster and lower IT costs. Architectures that do not leverage that breadth (e.g., if they use only Amazon EC2) might not be making the most of cloud computing and might be missing an opportunity to reduce costs and increase operational efficiency. AWS managed services provide building blocks that developers can consume to power their applications. These managed services include databases, machine learning, analytics, queuing, search, email, notifications, and more. For example, with Amazon SQS you can offload the administrative burden of operating a highly available, scalable messaging cluster, while paying a low price for only what you use. The same applies to Amazon S3, which enables you to store as much data as you want and access it when you need it, without having to think about capacity, hard disk configurations, replication, and other administrative issues.

"Migrate production workloads to AWS edge locations instead of AWS Regions" is incorrect. Edge locations do not have the compute, storage, networking required to run an entire workload. An Edge location is a site that CloudFront uses to cache copies of your content for faster delivery to users at any location.

"Use AWS Outposts to run all workloads in a cost-optimized environment" is incorrect. AWS Outposts is used by customers who must store and process data locally at their own data center. AWS Outposts allows customers to securely store and process customer data that needs to remain on-premises or in countries where there is no AWS region. This may help address requirements of companies in highly regulated industries and or those located in countries with data residency requirements. AWS Outposts is an AWS service that delivers the same AWS infrastructure, native AWS services, APIs, and tools to virtually any customer on-premises facility. With AWS Outposts, customers can run AWS services locally on their Outpost, including EC2, EBS, ECS, EKS, and Amazon RDS.

References:

<https://aws.amazon.com/ec2/dedicated-hosts/>

Question 62:

Skipped

An external auditor is requesting a log of all accesses to the AWS resources in the company's account. Which of the following services will provide the auditor with the requested information?



Amazon CloudFront



Amazon CloudWatch



AWS CloudTrail

(Correct)



AWS CloudFormation

Explanation

CloudTrail provides visibility into user activity by recording actions taken on your account. CloudTrail records important information about each action, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. This information helps you to enable governance, compliance, operational auditing, and risk auditing of your AWS account.

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

Amazon CloudWatch is incorrect. Amazon CloudWatch is used to monitor the utilization of the AWS cloud 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.

AWS CloudFormation is incorrect. AWS CloudFormation allows you to model your entire infrastructure with either a text file or programming languages, also referred to as infrastructure as code.

References:

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

Question 63:

Skipped

Which of the following is a type of MFA device that customers can use to protect their AWS resources?

-
- AWS Key Pair
-
- AWS CloudHSM
-
- AWS Access Keys
-
- U2F Security Key

(Correct)

Explanation

AWS multi-factor authentication (AWS MFA) provides an extra level of security that customers can apply to their AWS environment. 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 the AWS account resources. AWS supports several MFA device options including **Virtual MFA devices**, **Universal 2nd Factor (U2F) security key**, and **Hardware MFA devices**.

The other options are incorrect:

"Access Keys" is incorrect. Access keys are long-term credentials for an IAM user or the AWS account root user. Customers can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

"AWS Key Pair" is incorrect. The AWS Key pair cryptography enables customers to securely access their Amazon EC2 instances using a private key instead of a password.

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

References:

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

Question 64:

Skipped

How does AWS notify customers about security and privacy events pertaining to AWS services?

-
-

Using Compliance Resources

-
-

Using Security Bulletins

(Correct)

-
-

Using the AWS Management Console

-
-

Using the AWS ACM service

Explanation

AWS publishes security bulletins about the latest security and privacy events with AWS services on the Security Bulletins page.

The other options are incorrect:

"Using Compliance Resources" is incorrect. Compliance Resources offers guidance around achieving regulatory compliance on AWS. You can find more information about compliance resources here: <https://aws.amazon.com/compliance/>

"Using the AWS Management Console" is incorrect. The AWS Management Console is used to access AWS services, however security and privacy events are available - at the Security Bulletins page - without having to have an AWS account.

"Using the AWS ACM service" is incorrect. AWS Certificate Manager (ACM) 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/security/security-bulletins/>

Question 65:

Skipped

A customer is planning to migrate their Microsoft SQL Server databases to AWS. Which AWS Services can the customer use to run their Microsoft SQL Server database on AWS? (Choose TWO)

- Amazon Elastic Compute Cloud

(Correct)

- AWS Lambda
- Amazon RDS

(Correct)

- AWS Database Migration service (DMS)
- AWS Fargate

Explanation

Amazon Web Services offers the flexibility to run Microsoft SQL Server as either a self-managed component inside of EC2, or as a managed service via Amazon RDS. Using SQL Server on Amazon EC2 gives customers complete control over the database, just like when it's installed on-premises. Amazon RDS is a fully managed service where AWS manages the maintenance, backups, and patching.

The other options are incorrect:

AWS Database Migration Service (DMS) is incorrect. AWS Database Migration service (DMS) is an AWS Service designed to assist customers in migrating their databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from most widely used commercial and open-source databases. It is important to

note that while DMS can be used to **migrate the data**, it has nothing to do with **running** the database.

AWS Fargate is incorrect. AWS Fargate is a compute engine for Amazon Elastic Container Service (ECS) that allows customers to run containers without having to manage servers or clusters.

AWS Lambda is incorrect. AWS Lambda is a compute service that lets you run code without provisioning or managing servers (serverless).

References:

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

Question 1:

Skipped

For new AWS customers, what is the EASIEST way to launch a simple WordPress website on AWS?

-

Host the website directly on AWS Cloud Development Kit (AWS CDK)

-

Use the Amazon S3 Web hosting feature

-

Run WordPress on an Amazon Lightsail instance

(Correct)

-

Install WordPress on an Amazon EC2 instance

Explanation

Amazon Lightsail is designed to be the easiest way to launch and manage a Web server using AWS. Lightsail plans include everything you need to jumpstart your project – a virtual machine, SSD-based storage, data transfer, DNS management, and a static IP address – for a low, predictable price.

Amazon Lightsail is best for Websites built on common applications like WordPress, Joomla, Drupal, Magento. You can get started using Lightsail for your website with just a few clicks. Choose the operating system or application template that's best for your website, and your virtual private server is ready in less than a minute. You can easily manage your web server, DNS, and IP addresses directly from the Lightsail console.

The other options are incorrect:

"Use the Amazon S3 web hosting feature" is incorrect. The Amazon S3 web hosting feature enables you to host static websites only. You cannot use Amazon S3 to host dynamic websites such as WordPress websites.

A dynamic website relies on server-side processing, and it uses server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting and cannot be used to host dynamic websites.

"Install WordPress on an Amazon EC2 instance" is incorrect. Installing WordPress on an Amazon EC2 instance is not the easiest way to launch a WordPress website, especially for customers who are new to AWS. To learn more about how to use Amazon EC2 to host a WordPress website, visit this page: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/hosting-wordpress.html>

"Host the website directly on AWS Cloud Development Kit (AWS CDK)" is incorrect. AWS Cloud Development Kit (AWS CDK) is not used for web hosting. The AWS Cloud Development Kit (AWS CDK) is an open-source software development framework for defining cloud infrastructure as code with modern programming languages and deploying it through AWS CloudFormation. AWS CDK enables you to use your existing programming skills and tools, and apply those to the task of building cloud infrastructure. AWS CDK is generally available in JavaScript, TypeScript, Python, Java, and C#.

You can think of the AWS CDK as a developer-centric toolkit that leverages the full power of modern programming languages to define your AWS infrastructure as code. The CDK actually builds on AWS CloudFormation and uses it as the engine for provisioning AWS resources. Rather than using a declarative language like JSON or YAML to define your infrastructure (as is the case with CloudFormation), the CDK lets you do that in your favorite imperative programming language. This includes languages such as JavaScript, TypeScript, Java, C#, and Python. When AWS CDK applications are run, they compile down to fully formed CloudFormation JSON/YAML templates that are then submitted to the CloudFormation service for provisioning.

References:

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

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

Question 2:

Skipped

Your application requirements for CPU and RAM are changing in an unpredictable way. Which service can be used to dynamically adjust these resources based on load?



Amazon Route53



ELB



Auto Scaling

(Correct)



Amazon Elastic Container Service

Explanation

AWS Auto Scaling is a service that can help you optimize your utilization and cost efficiencies when consuming AWS services so you only pay for the resources you actually need. When demand decreases, Auto Scaling shuts down unused resources automatically to reduce costs. When demand increases, Auto Scaling provisions new resources automatically to meet demand and maintain performance.

The other options are incorrect:

ELB is incorrect. Elastic Load Balancing (ELB) is used to distribute traffic automatically across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.

Amazon Route53 is incorrect. Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service.

Amazon Elastic Container Service is incorrect. Amazon Elastic Container Service is used to run containerized applications in AWS.

References:

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

Question 3:

Skipped

Which of the following strategies helps protect your AWS root account?

- Access the root account only from your personal Mobile Phone
- Delete root user access keys if you do not need them

(Correct)

- Only share your AWS account password or access keys with trusted persons
- Apply MFA for the root account and use it for all of your work

Explanation

Anyone who has root user access keys for your AWS account has unrestricted access to all the resources in your account, including billing information. If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. If you do have an access key for your AWS account root user, **delete it**. If you must keep it, rotate (change) the access key regularly.

There are specific tasks that are restricted to the AWS account root user. For example, only the root user can perform the following tasks: **(IMPORTANT)**

- 1- Change your account settings. This includes the account name, root user password, and email address.
- 2- View certain tax invoices.
- 3- Close your AWS account.
- 4- Change your AWS Support plan or Cancel your AWS Support plan.

5- Activate IAM access to the Billing and Cost Management console. By default, IAM users and roles within an AWS account can't access the Billing console pages. The AWS account root user can allow IAM users and roles access to Billing console pages by using the **Activate IAM Access** setting.

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

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

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

The other options are incorrect:

"Access the root account only from your personal Mobile Phone" is incorrect. You can access your root account from any supported device, but make sure that no one else can access these devices or monitor them.

"Only share your AWS account password or access keys with trusted persons" is incorrect. You should never share your AWS account password or access keys with anyone. Instead, create individual named users for anyone who needs access to your AWS account. By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions any time. (If you give out your root user credentials, it can be difficult to revoke them, and it is impossible to restrict their permissions.).

Additional information:

Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (administrators, developers, accounting, etc.). Next, define the relevant permissions for each group. Finally, assign IAM users to those groups. All the users in an IAM group inherit the permissions assigned to the group. That way, you can make changes for everyone in a group in just one

place. As people move around in your company, you can simply change what IAM group their IAM user belongs to.

"Apply MFA for the root account and use it for all of your work" is incorrect. AWS strongly recommends that you do not use the AWS account root user for day-to-day tasks, even administrative tasks. Instead, use the root user to create your first IAM user, then use this instead. Securely lock away the root user credentials and only use them for tasks that require root access.

References:

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

Question 4:

Skipped

What does the Amazon CloudFront service provide? (Choose TWO)

- Simplifies online data migrations from on-premises data centers to AWS
- Enables faster disaster recovery

Increases application availability by caching at the edge

(Correct)

- Tracks user activity and API usage
- Delivers content to end users with low latency

(Correct)

Explanation

"Delivers content to end users with low latency" is correct. Amazon CloudFront employs a global network of edge locations and regional edge caches that cache copies of your content close to your end-users. Amazon CloudFront ensures that end-user requests are serviced by the closest edge location. As a result, requests travel a short distance, improving performance for your end-users.

"Increases application availability by caching at the edge" is correct. Web applications often need to contend with spikes in traffic during peak periods of activity. By using Amazon CloudFront, you can cache your content in CloudFront's edge locations worldwide and reduce the workload on your origin by only fetching content from your origin when needed. This reduced workload on your origin helps you increase the availability of your application.

Note: An origin server is the server that holds the original, definitive versions of your content.

The other options are incorrect:

"Simplifies online data migrations from on-premises data centers to AWS" is incorrect. Amazon CloudFront is not for online data migrations. Amazon CloudFront is a content delivery network. The name of the service that can be used for online data migrations from on-premises data centers to AWS is **AWS DataSync**.

AWS DataSync is an online data transfer service that simplifies, automates, and accelerates copying large amounts of data between on-premises storage systems and AWS Storage services, as well as between AWS Storage services. AWS DataSync reduces the complexity and cost of online data transfer, making it simple to transfer datasets between on-premises storage systems and AWS Storage services, and between AWS Storage services.

"Enables faster disaster recovery" is incorrect. CloudFront is not used for disaster recovery. It is used to serve content with low latency by caching copies of objects close to your end-users.

Disaster recovery is about preparing for and recovering from a disaster. Any event that has a negative impact on your business continuity or finances could be termed a disaster. This could be hardware or software failure, a network outage, a power outage, physical damage to a building like fire or flooding, human error, or some

other significant disaster. In AWS, customers have the flexibility to choose the right approach that fits their budget. The approaches could be as minimum as backup and restore from the cloud or full-scale multi-site solution deployed in onsite and AWS with data replication and mirroring. Read more about disaster recovery here: <https://aws.amazon.com/blogs/publicsector/rapidly-recover-mission-critical-systems-in-a-disaster/>

"Tracks user activity and API usage" is incorrect. Amazon CloudTrail is the service that can be used to track user activity and API usage.

References:

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

Question 5:

Skipped

What are some key design principles for designing public cloud systems? (Choose TWO)

- Disposable resources instead of fixed servers

(Correct)

- Servers instead of managed services
- Loose coupling over tight coupling

(Correct)

- Reserved capacity instead of on demand
- Multi-AZ deployments instead of multi-region deployments

Explanation

The AWS Cloud includes many design patterns and architectural options that you can apply to a wide variety of use cases. Some key design principles of the AWS Cloud include scalability, disposable resources, automation, loose coupling, managed services instead of servers, and flexible data storage options.

Disposable resources instead of fixed servers:

When designing for the cloud, you can think of servers and other components as temporary resources that you can provision only when you need them instead of fixed servers that exist all the time. This approach solves many problems that usually appear in traditional, on-premises environments. For example, changes and software patches applied over time to the same (fixed) server can result in untested and heterogeneous configurations across different environments. You can solve this problem in AWS with an immutable infrastructure pattern. With this approach, if a problem happens with a server (EC2 instance), rather than updating, it is replaced with a new server containing the latest patches and configuration. This enables resources to always be in a consistent (and tested) state and makes rollbacks easier to perform.

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 systems and applications 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.

The other options are incorrect:

"Servers instead of managed services" is incorrect. AWS recommend the use of managed services instead of servers where possible. AWS offers a broad set of compute, storage, database, analytics, application, and deployment services that help organizations move faster and lower IT costs. Architectures that do not leverage that breadth (e.g., if they use only Amazon EC2) might not be making the most of cloud

computing and might be missing an opportunity to increase developer productivity and operational efficiency. AWS managed services provide building blocks that developers can consume to power their applications. These managed services include databases, machine learning, analytics, queuing, search, email, notifications, and more. For example, with Amazon SQS you can offload the administrative burden of operating a highly available, scalable messaging cluster, while paying a low price for only what you use. The same applies to Amazon S3, which enables you to store as much data as you want and access it when you need it, without having to think about capacity, hard disk configurations, replication, and other administrative issues.

"Reserved capacity instead of on demand" is incorrect. Each instance pricing model has its own use case. The on-demand option is best suited for the applications with short-term, spiky, or unpredictable workloads. The Reserved option is best suited for the applications that have steady state usage for long periods of time.

"Multi-AZ deployments instead of multi-region deployments" is incorrect. If you have users from all around the world, you should deploy in multiple regions or use the CloudFront service to reduce latency to those users. You may also choose to deploy in more than one region for disaster recovery.

References:

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

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

Question 6:

Skipped

To protect against data loss, you need to backup your database regularly. What is the most cost-effective storage option that provides immediate retrieval of your backups?

-
-

Amazon S3 Glacier

-
-

Amazon S3 Standard-Infrequent Access

(Correct)



Amazon S3 Glacier Deep Archive



Instance Store

Explanation

Amazon S3 has a wide variety of storage classes to cover different workloads and use cases. The S3 storage class you choose primarily depends upon two factors: accessibility and cost. If you need **immediate access** to your data, then you want to use either S3 Standard, S3 Intelligent-Tiering, **S3 Standard-Infrequent Access**, or S3 One Zone-IA. If you don't require regular and immediate access to your data, then S3 Glacier or S3 Glacier Deep Archive may be a good choice. The S3 Glacier storage classes have an overall lower cost than the S3 storage classes that provide immediate access to your data.

Database backup is an important operation to consider for any database system. Taking backups not only enables data restore on database failure but also enables recovery from data corruption. Amazon S3 Standard-Infrequent Access is the best choice because it provides **immediate access** to your database backups while reducing costs. S3 Standard-IA is ideal for data that is accessed less frequently (like database backups), but requires immediate access when needed.

The other options are incorrect:

"Amazon S3 Glacier" is incorrect. Amazon Glacier does not provide immediate retrieval. Amazon Glacier provides three options to retrieve your data with retrieval times ranging from a few minutes to several hours. Amazon Glacier is a low-cost S3 storage class for data archiving.

"Amazon S3 Glacier Deep Archive" is incorrect. Amazon S3 Glacier Deep Archive does not provide immediate retrieval. With S3 Glacier Deep Archive, the minimum retrieval period is 12 hours. S3 Glacier Deep Archive is Amazon S3's lowest-cost

storage class that supports long-term retention and digital preservation for data that may be accessed once or twice in a year.

Note: Choosing between S3 Glacier and S3 Glacier Deep Archive depends on how quickly you must retrieve your data. With S3 Glacier, you can retrieve your data within a few minutes to a few hours, whereas with S3 Glacier Deep Archive, the minimum retrieval period is 12 hours.

"Instance Store" is incorrect. Instance Store can only be used to store temporary data such as buffers, caches, scratch data, and other temporary content. You cannot rely on instance store for valuable, long-term data because data in the instance store is lost if the instance stops, terminates or if the underlying disk drive fails.

References:

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

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

Question 7:

Skipped

Which of the following AWS services would help you migrate on-premise databases to AWS?

- Amazon S3 Transfer Acceleration

- AWS DMS

(Correct)

- AWS Transit Gateway
- AWS Directory Service

Explanation

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

The other options are incorrect:

AWS Directory Service is incorrect. AWS Directory Service is a managed Microsoft Active Directory in the AWS Cloud. Customers can use it to manage users and groups, provide single sign-on (SSO) to applications and services, as well as create and apply group policies.

Note: What is Single sign-on (SSO)? AWS Single sign-on (AWS SSO) enables a company's employees to sign in to AWS using their existing corporate Microsoft Active Directory credentials.

Amazon S3 Transfer Acceleration is incorrect. Amazon S3 Transfer Acceleration helps to read and write data to Amazon S3 over long geographic distances with low latency.

AWS Transit Gateway is incorrect. AWS Transit Gateway is a network transit hub that customers can use to interconnect their virtual private clouds (VPCs) and their on-premises networks. AWS transit gateway simplifies how customers interconnect all of their VPCs, across thousands of AWS accounts and into their on-premises networks.

References:

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

Question 8:

Skipped

Which of the following is a cloud computing deployment model that connects infrastructure and applications between cloud-based resources and existing resources not located in the cloud?

Cloud

On-premises

Mixed

Hybrid

(Correct)

Explanation

A hybrid cloud model connects infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud. The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend, and grow, an organization's infrastructure into the cloud while connecting cloud resources to internal systems.

The other options are incorrect:

Cloud is incorrect. A cloud-based application is fully deployed in the cloud and all parts of the application run in the cloud. Applications in the cloud have either been created in the cloud or have been migrated from an existing infrastructure to take advantage of the benefits of cloud computing. The most famous Cloud Computing providers are Amazon AWS, Microsoft Azure, and Google Cloud.

On-premises is incorrect. An on-premises model is where an organization has their infrastructure and applications running in a datacenter that they own, or on hardware they are leasing from a third-party provider in their datacenter.

Mixed is incorrect. There are only three Cloud Computing deployment models: Cloud, Hybrid, and On-premises.

References:

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

Question 9:

Skipped

A developer wants to quickly deploy and manage his application in the AWS Cloud, but he doesn't have any experience with cloud computing. Which of the following AWS services would help the developer achieve his goal?

- AWS Elastic Beanstalk
- **(Correct)**
- AWS Fargate
- AWS Amplify
- Amazon Personalize

Explanation

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

The other options are incorrect:

Amazon Personalize is incorrect. Amazon Personalize is a fully managed machine learning service that can be used to deliver highly customized recommendations to customers across industries such as retail, media and entertainment. Amazon Personalize enables developers to build applications with the same machine learning (ML) technology used by Amazon.com for real-time personalized recommendations. Amazon Personalize can be used to personalize the end-user experience over any digital channel. Examples include product recommendations for e-commerce, news articles and content recommendation for publishing, media and social networks, hotel recommendations for travel websites, and credit card recommendations for banks.

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

AWS Amplify is incorrect. AWS Amplify is not for **deploying** applications. AWS Amplify is used to **build** secure and scalable web and mobile applications. AWS Amplify consists of a set of tools (open-source framework, admin UI, console) and services that makes it quick and easy for front-end web and mobile developers build full-stack applications on AWS, with the flexibility to leverage the breadth of AWS services to further customize applications. Amplify supports popular languages, frameworks, and platforms, including JavaScript, React, Angular, Vue, and Next.js for web apps, and Android, iOS, React Native, Ionic, and Flutter for mobile apps.

References:

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

Question 10:

Skipped

What does AWS Cost Explorer provide to help manage your spend?

-
-

Detailed reports about the utilization of on-premises servers

-
-

Accurate estimates of AWS service costs based on your expected usage

-

Highly accurate cost forecasts for up to 12 months ahead

(Correct)

-

Consolidated billing

Explanation

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

Cost Explorer's cost forecast capabilities use machine learning to learn each customer's historical spend patterns and use that information to forecast expected costs. Cost Explorer's forecasting enables you to get a better idea of what your costs and usage may look like in the future, so that you can plan ahead. Customers can use AWS Cost Explorer to estimate their cost and usage in a custom time range within the next **3 months (DAILY forecasts)** or within the next **12 months (MONTHLY forecasts)**.

The other options are incorrect:

"Accurate estimates of AWS service costs based on your expected usage" is incorrect. AWS Cost Explorer forecasts your future costs based on your past usage; NOT based on your expected usage. The AWS tool that can provide accurate estimates of AWS service costs based on your expected usage is the AWS Pricing Calculator. For example, if you are planning to use 500 GB of S3 storage, you can input this value directly in the AWS Pricing Calculator interface and the calculator provides an estimate of what you will pay monthly for this amount of storage.

"Detailed reports about the utilization of on-premises servers" is incorrect. AWS Cost Explorer does not provide reports about the utilization of your on-premises servers. AWS Cost Explorer provides reports about your overall Amazon EC2 usage and a detailed report about the utilization of Amazon EC2 Reserved Instances.

"Consolidated billing" is incorrect. Consolidated billing is a feature in AWS Organizations that enables you to consolidate billing and payment for multiple AWS accounts.

References:

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

<https://aws.amazon.com/about-aws/whats-new/2018/11/enhanced-forecasting-now-available-in-aws-cost-explorer/>

Question 11:

Skipped

For Amazon RDS databases, what does AWS perform on your behalf? (Choose TWO)

- Access management
- Management of the operating system

(Correct)

- Management of firewall rules
- Network traffic protection
- Database setup

(Correct)

Explanation

In relation to Amazon RDS databases:

AWS is responsible for:

- 1- Managing the underlying infrastructure and foundation services.
- 2- Managing the operating system.
- 3- Database setup.
- 4- Patching and backups.

The customer is still responsible for:

- 1- Protecting the data stored in databases (through encryption and IAM access control).
- 2- Managing the database settings that are specific to the application.
- 3- Building the relational schema.
- 4- Network traffic protection.

The other options are incorrect:

"Access management" is incorrect. The customer is responsible for managing access to all AWS services and resources.

"Management of firewall rules" is incorrect. The customer is responsible for managing firewall rules using security groups.

"Network traffic protection" is incorrect. The customer is responsible for protecting network traffic using security groups, Network ACLs and AWS WAFs.

References:

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

Question 12:

Skipped

Which of the following are factors should be considered for Amazon EBS pricing?
(Choose TWO)

-

The compute capacity you consume

-

The amount of data you have stored in snapshots

(Correct)

-

The number of Snowball storage devices you request

-

The size of volumes provisioned per month

(Correct)

-

The compute time you consume

Explanation

Amazon EBS pricing has two factors:

1- Volumes: Volume storage for all EBS volume types is charged by the amount of GB you provision per month, until you release the storage.

2- Snapshots: Snapshot storage is based on the amount of space your data consumes in Amazon S3. Because Amazon EBS does not save empty blocks, it is likely that the snapshot size will be considerably less than your volume size. Copying EBS snapshots is charged based on the volume of data transferred across regions. For the first snapshot of a volume, Amazon EBS saves a full copy of your data to Amazon S3. For each incremental snapshot, only the changed part of your Amazon EBS volume is saved. After the snapshot is copied, standard EBS snapshot charges apply for storage in the destination region.

The other options are incorrect:

"The compute capacity you consume" and "The compute time you consume" are incorrect. Amazon EBS is not a compute service.

"The number of Snowball storage devices you request" is incorrect. There is no relation between Amazon EBS and AWS Snowball. AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS using storage devices designed to be secure for physical transport. Using Snowball helps to eliminate challenges that can be encountered with large-scale data transfers including high network costs, long transfer times, and security concerns.

References:

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/how-aws-pricing-works.pdf> page 12

Question 13:

Skipped

An organization uses a hybrid cloud architecture to run their business. Which AWS service enables them to deploy their applications to any AWS or on-premises server?

- AWS CodeDeploy
- **(Correct)**
- Amazon QuickSight
- Amazon Athena
- Amazon Kinesis

Explanation

AWS CodeDeploy is a service that automates application deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone manual operations, and the service scales with your infrastructure so you can easily deploy to one instance or thousands.

You can also use AWS OpsWorks to automate application deployments to any instance, including Amazon EC2 instances and instances running on-premises. OpsWorks is a service that helps you automate operational tasks like code deployment, software configurations, package installations, database setups, and server scaling using Chef and Puppet.

The other options are incorrect:

"Amazon Athena" is incorrect. Amazon Athena is an analytics service that makes it easy to query data in Amazon S3 using standard SQL commands. AWS customers can also use an Amazon S3 feature called **S3 Select** to query data on S3 using SQL commands; however, S3 Select can only be used to perform simple SQL queries on a single S3 Object.

"Amazon Kinesis" is incorrect. Amazon Kinesis is an analytics service that allows you to easily collect, process, and analyze video and data streams in real time.

"Amazon QuickSight" is incorrect. Amazon QuickSight is a machine learning-powered business intelligence (BI) service built for the cloud. QuickSight lets you easily create and publish **interactive BI dashboards** that include Machine Learning-powered insights. QuickSight dashboards can be accessed from any device, and seamlessly embedded into your applications, portals, and websites.

Unlike traditional BI or data discovery solutions, getting started with Amazon QuickSight is simple and fast. When you log in, Amazon QuickSight seamlessly discovers your data sources in AWS services such as Amazon Redshift, Amazon RDS, Amazon Athena, and Amazon Simple Storage Service (Amazon S3). You can connect to any of the data sources discovered by Amazon QuickSight **and get insights from this data in minutes.** Amazon QuickSight supports rich data discovery and business

analytics capabilities to help customers derive valuable insights from their data without worrying about provisioning or managing infrastructure.

References:

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

<https://aws.amazon.com/about-aws/whats-new/2015/04/aws-codedeploy-supports-on-premises-instances/>

<https://aws.amazon.com/about-aws/whats-new/2014/12/08/aws-opsworks-supports-existing-ec2-instances-and-on-premises-servers/>

Question 14:

Skipped

A company wants to replace its traditional desktops with Cloud desktops and enable Work-From-Home for its employees. The virtualized desktops must be persistent and can be accessed from anywhere. Which AWS service will meet these requirements?



Amazon AppStream 2.0



AWS Local Zones



Amazon WorkSpaces

(Correct)



AWS Wavelength Zones

Explanation

An Amazon WorkSpace is a cloud-based virtual desktop that can act as a replacement for a traditional desktop. A WorkSpace is available as a bundle of operating system, compute resources, storage space, and software applications that allow a user to perform day-to-day tasks just like using a traditional desktop. With Amazon WorkSpaces, your employees get a fast, responsive desktop of their choice that they can access anywhere, anytime, from any supported device. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few

minutes and quickly scale to provide thousands of desktops to workers across the globe.

The other options are incorrect:

"Amazon AppStream 2.0" is incorrect. Amazon AppStream 2.0 lets you move your desktop applications to AWS, without rewriting them. Amazon AppStream 2.0 is a fully managed non-persistent application and desktop streaming service that provides users instant access to their desktop applications from anywhere. Amazon AppStream 2.0 simplifies application management, improves security, and reduces costs by moving a company's applications from their users' physical devices to the AWS Cloud.

While AppStream 2.0 helps you move your existing **desktop applications** to AWS, so users can access them from anywhere, Amazon Workspaces provides an **entire virtual Desktop** that can act as a replacement for a traditional desktop.

"AWS Wavelength Zones" is incorrect. Wavelength Zones are AWS infrastructure deployments that embed AWS compute and storage services within telecommunications providers' datacenters at the edge of the 5G network, so application traffic can reach application servers running in Wavelength Zones without leaving the mobile providers' network. This prevents the latency that would result from multiple hops to the Internet and enables customers to take full advantage of 5G networks. Wavelength Zones extend AWS to the 5G edge, delivering a consistent developer experience across multiple 5G networks around the world and allowing developers to build the next generation of ultra-low latency applications using the same familiar AWS services, APIs, tools, and functionality they already use today.

"AWS Local Zones" is incorrect. A Local Zone is an extension of an AWS Region in geographic proximity to your users. With AWS Local Zones, you can easily run highly-demanding applications that require single-digit millisecond latencies to your end-users, such as real-time gaming, hybrid migrations, AR/VR, and machine learning.

References:

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

Question 15:

Skipped

Why are Serverless Architectures more economical than Server-based Architectures?

- With the Server-based Architectures, compute resources continue to run all the time but with serverless architecture, compute resources are only used when code is being executed

(Correct)

- When you reserve serverless capacity, you will get large discounts compared to server reservation
- Serverless Architectures use new powerful computing devices
- With Serverless Architectures you have the ability to scale automatically up or down as demand changes

Explanation

Serverless architectures can reduce costs because you do not have to manage or pay for underutilized servers, or provision redundant infrastructure to implement high availability. For example, you can upload your code to the AWS Lambda compute service, and the service can run the code on your behalf using AWS infrastructure. With AWS Lambda, you are charged for every 100ms your code executes and the number of times your code is triggered.

The other options are incorrect:

"Serverless Architectures use new powerful computing devices" is incorrect. AWS uses the same devices for both server-based and serverless architectures.

"With Serverless Architectures you have the ability to scale automatically up or down as demand changes" is incorrect. With Serverless Architecture, you do not have to worry about scaling compute capacity. AWS handles that for you.

"When you reserve serverless capacity, you will get large discounts compared to server reservation" is incorrect. There are no reservations when using Serverless Architectures.

References:

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

Question 16:

Skipped

Your CTO has asked you to contact AWS support using the chat feature to ask for guidance related to EBS. However, when you open the AWS support center you can't see a way to contact support via Chat. What should you do?

-
-

Upgrade from the Basic Support plan to Developer Support

-
-

The chat feature is available for all plans for an additional fee, but you have to request it first

-
-

At a minimum, upgrade to Business support plan

(Correct)

-
-

There is no chat feature in AWS support

Explanation

Chat access to AWS Support Engineers is available at the Business and Enterprise support tiers only.

References:

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

Question 17:

Skipped

You need to migrate a large number of on-premises workloads to AWS. Which AWS service is the most appropriate?

- AWS File Transfer Acceleration
- AWS Server Migration Service
- **(Correct)** AWS Application Discovery Service
- AWS Database Migration Service

Explanation

AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for you to migrate thousands of on-premises workloads to AWS. AWS SMS allows you to automate, schedule, and track incremental replications of live server volumes, making it easier for you to coordinate large-scale server migrations.

AWS Server Migration Service currently supports virtual machine migrations from VMware vSphere, Windows Hyper-V, or Microsoft Azure to AWS. Each server volume migrated is saved as a new Amazon Machine Image (AMI), which can be launched as an EC2 instance (virtual machine) in the AWS cloud.

The other options are incorrect:

"AWS Database Migration Service" is incorrect. AWS Database Migration Service is used to migrate your data to and from most of the widely used commercial and open source databases.

"AWS Application Discovery Service" is incorrect. AWS Application Discovery Service is used to discover on-premises server inventory and behavior. This service is very useful when creating a migration plan to AWS.

"AWS File Transfer Acceleration" is incorrect. AWS File Transfer Acceleration is an S3 feature that enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket.

References:

<https://aws.amazon.com/server-migration-service/>

Question 18:

Skipped

Which AWS service helps developers compile and test their code?



AWS CodeBuild

(Correct)



AWS CodeCommit



AWS CodeDeploy



CloudEndure

Explanation

AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy.

AWS CodeCommit vs. AWS CodeBuild vs. AWS CodeDeploy vs. AWS CodePipeline:

- AWS CodeCommit is used to **store and version** source code.
- AWS CodeBuild is used to **compile and test** source code, helping you find and fix bugs early in the development process when they are easy to fix.
- AWS CodeDeploy is used to **deploy** application code to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers.
- AWS CodePipeline is the glue that builds these steps together. AWS CodePipeline enables you to **automate all phases of your release process**, from committing the code into AWS CodeCommit all the way to deploying it with AWS CodeDeploy. You can also integrate your own custom tools into any stage of the release process to form an end-to-end continuous delivery solution. This enables you to deliver new features and updates rapidly and reliably.

The other options are incorrect:

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

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

"CloudEndure" is incorrect. There are two CloudEndure services:

1- CloudEndure Migration: CloudEndure Migration is a highly automated lift-and-shift (rehost) solution that simplifies the process of migrating applications from

physical, virtual, and cloud-based infrastructure, ensuring that they are fully operational in any AWS Region without compatibility issues.

2- CloudEndure Disaster Recovery: CloudEndure Disaster Recovery is a disaster recovery solution that minimizes downtime and data loss by providing fast, reliable recovery of physical, virtual, and cloud-based servers into AWS Cloud. CloudEndure Disaster Recovery continuously replicates your machines (including operating system, system state configuration, databases, applications, and files) into a low-cost staging area in your target AWS account and preferred Region. In the case of a disaster (e.g., power failure, cyber-attack), you can instruct CloudEndure Disaster Recovery to automatically launch thousands of your machines in their fully provisioned state in minutes.

References:

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

Question 19:

Skipped

You want to transfer 200 Terabytes of data from on-premises locations to the AWS Cloud, which of the following can do the job in a cost-effective way?

- AWS DataSync
- AWS DMS
- AWS Snowball

(Correct)

- AWS Snowmobile

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. 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 devices provides up to 80 TB of usable storage.

In our case, it is better (cost-effective) to use 3 snowball Edge Storage Optimized devices to transfer 200 TB instead of using the internet.

$$3 \text{ snowballs} * 80\text{TB} = 240 \text{ TB}$$

There are many options for transferring your data into AWS. Snowball is intended for transferring large amounts of data. If you want to transfer less than 10 terabytes of data between your on-premises data centers and Amazon S3, Snowball might not be your most economical choice.

The other options are incorrect:

AWS DataSync is incorrect. AWS DataSync is ideal for online data transfers, not offline data transfers. You can use DataSync to migrate **active data** from on-premises locations to AWS, transfer data to the cloud for analysis and processing,

archive data to free up on-premises storage capacity, or replicate data to AWS for business continuity.

AWS Snowmobile is incorrect. Snowmobile is not a cost effective solution here. AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to 100 Petabytes (100,000 Terabytes) per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck.

AWS DMS is incorrect. AWS Database Migration Service (DMS) is used to migrate databases to AWS.

References:

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

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

Question 20:

Skipped

Which of the following compute resources are serverless? (Choose TWO)

-

Amazon ECS

-

Amazon EMR

-

Amazon EC2

-

AWS Lambda

(Correct)



AWS Fargate

(Correct)

Explanation

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume, and there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability.

AWS Fargate is a compute engine for deploying and managing containers, which frees you from having to manage any of the underlying infrastructure. With AWS Fargate, you no longer have to provision, configure, and scale clusters of virtual machines to run containers. AWS Fargate seamlessly integrates with Amazon ECS, so you can deploy and manage containers without having to provision or manage servers.

The other options are incorrect:

Amazon EC2 is incorrect. Amazon EC2 provides its compute capacity through instances (servers).

Amazon EMR is incorrect. Amazon EMR is not serverless. Amazon EMR uses Amazon EC2 to process data at any scale.

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

References:

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

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

Question 21:

Skipped

Which of the following services allows you to install and run custom relational database software?

- Amazon Cognito
- Amazon Inspector
- Amazon EC2
- (Correct)**
- Amazon RDS

Explanation

If an AWS customer needs full control over a database, AWS provides a wide range of Amazon EC2 instances - with different hardware characteristics - on which they can install and run their custom relational database software.

If EC2 is used instead of RDS to run a relational database, the customer is responsible for managing everything related to this database.

The other options are incorrect:

"Amazon Inspector" is incorrect. Amazon Inspector is a security assessment service that automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

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

"Amazon RDS" is incorrect. Amazon RDS provides **six database engines** to choose from, including **Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and Microsoft SQL Server**. These engines are already installed and ready to be used. The customer does not install the actual database software on RDS, nor has access to the underlying host as it is a managed service.

References:

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

Question 22:

Skipped

You have migrated your application to AWS recently. How can you view the AWS costs applied to your account?

-
-

Using the Amazon AppStream 2.0 dashboard

-
-

Using the AWS CloudWatch logs dashboard

-
-

Using the AWS Cost & Usage Report

(Correct)

-
-

Using the Amazon VPC dashboard

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:

"Using the Amazon AppStream 2.0 dashboard" is incorrect. Amazon AppStream 2.0 doesn't provide any cost information. AppStream 2.0 helps you move your existing desktop applications to AWS so that users can access them from anywhere.

Interactively streaming your application from the cloud provides several benefits:

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

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

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

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

"Using the AWS CloudWatch logs dashboard" is incorrect. You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources. CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis. By default, logs are kept indefinitely and never expire. You can adjust the retention policy for each log group, keeping the indefinite retention, or choosing a retention periods between 10 years and one day.

"Using the Amazon VPC dashboard" is incorrect. Amazon VPC dashboard doesn't provide any cost information.

References:

<https://aws.amazon.com/aws-cost-management/aws-cost-and-usage-reporting/>

Question 23:

Skipped

Which of the following are valid Amazon EC2 Reserved Instance types? (Choose TWO)

- Bulk
- Standard

(Correct)

- Expedited
- Spot
- Convertible

(Correct)

Explanation

When you purchase a Reserved Instance, you can choose between a Standard or Convertible offering class.

Standard RIs: These provide the most significant discount (up to 72% off On-Demand) and are best suited for steady-state usage.

Convertible RIs: These provide a discount (up to 54% off On-Demand) and the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value. Like Standard RIs, Convertible RIs are best suited for steady-state usage.

Note: **Scheduled RIs** are no longer available in AWS.

The other options are incorrect:

Spot is incorrect. Spot is a different Amazon EC2 payment option.

Bulk and Expedited are incorrect. Bulk and Expedited are retrieval options for Amazon Glacier.

References:

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

Question 24:

Skipped

Which statement best describes the AWS Pay-As-You-Go pricing model?

-
-

With AWS, you replace large capital expenses with low variable payments

(Correct)

-
-

With AWS, you replace low upfront expenses with large fixed payments

-
-

With AWS, you replace low upfront expenses with large variable payments

-

With AWS, you replace large upfront expenses with low fixed payments

Explanation

AWS does not require minimum spend commitments or long-term contracts. You replace large fixed upfront expenses with low variable payments that only apply based on what you use. For example, when using On-demand instances you pay only for the hours\seconds they are running and nothing more.

References:

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

Question 25:

Skipped

Which of the below options are use cases of the Amazon Route 53 service? (Choose TWO)

-

Manages global application traffic through a variety of routing types

(Correct)

-

DNS configuration and management

(Correct)

-

Detects configuration changes in the AWS environment

-

Point-to-point connectivity between an on-premises data center and AWS

-

Provides infrastructure security optimization recommendations

Explanation

Amazon Route 53 can be used for:

- Registering domain names
- DNS configuration and management
- Configuring health checks to route traffic only to healthy endpoints
- Managing global application traffic (cross-regions) through a variety of routing types.

Amazon Route53 allows for registration of new domain names in AWS. Amazon Route 53 is a global service that provides a highly available and scalable Domain Name System (DNS) in the Cloud. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other.

Amazon Route 53 also offers health checks to monitor the health and performance of your application as well as your web servers and other resources. Route 53 can be configured to route traffic only to the healthy endpoints to achieve greater levels of fault tolerance in your applications.

Amazon Route 53 provides many routing types to help AWS Customers improve their application's performance for a global audience. For example, Amazon Route 53 latency-based policy routes user requests to the closest AWS Region, which reduces latency and improves application performance.

Amazon 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:

"Provides infrastructure security optimization recommendations" is incorrect. Route 53 does not provide infrastructure security optimization recommendations. The name of the service that performs this function is AWS Trusted Advisor.

"Detects configuration changes in the AWS environment" is incorrect. Route 53 is not used to detect configuration changes in the AWS environment. The name of the service that performs this function is AWS Config.

"Point-to-point connectivity between an on-premises data center and AWS" is incorrect. Route 53 does not provide point-to-point connectivity between an on-premises data center and AWS. The name of the service that performs this function is AWS Direct Connect.

References:

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

Question 26:

Skipped

Which of the following is a feature of Amazon RDS that performs automatic failover when the primary database fails to respond?



RDS Write Replica



RDS Multi-AZ

(Correct)



RDS Snapshots



RDS Single-AZ

Explanation

When you enable Multi-AZ, Amazon Relational Database Service (Amazon RDS) maintains a redundant and consistent standby copy of your data. If you encounter problems with the primary copy, Amazon RDS automatically switches to the standby copy (or to a read replica in the case of Amazon Aurora) to provide continued availability to the data. The two copies are maintained in different Availability Zones (AZs), hence the name "Multi-AZ." Each AZ runs on its own

physically distinct, independent infrastructure, and is engineered to be highly reliable. Having separate Availability Zones greatly reduces the likelihood that both copies will concurrently be affected by most types of disturbances.

The other options are incorrect:

"RDS Snapshots" is incorrect. RDS snapshots are user-initiated backups of your instance.

"RDS Write Replica" is incorrect. The name of this feature is RDS Read Replica, not RDS Write Replica. Amazon RDS can be configured to use Read Replicas to scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

"RDS Single-AZ" is incorrect. RDS Single-AZ is not an Amazon RDS feature.

References:

<https://aws.amazon.com/rds/details/multi-az/>

Question 27:

Skipped

What best describes penetration testing?

- Testing your instances to check for the unhealthy ones
 - Testing your network to find security vulnerabilities that an attacker could exploit
- (Correct)**
-

Testing your application's response time from different locations

-

Testing your software for bugs and errors

Explanation

Penetration testing is the practice of testing a network or web application to find security vulnerabilities that an attacker could exploit.

References:

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

Question 28:

Skipped

Which of the following would you use to manage your encryption keys in the AWS Cloud? (Choose TWO)

-

AWS Certificate Manager

-

AWS KMS

(Correct)

-

CloudHSM

(Correct)

-

AWS CodeDeploy

-

AWS CodeCommit

Explanation

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

FIPS 140-2 validated hardware security modules to protect the security of your keys. AWS Key Management Service is integrated with most other AWS services to help you protect the data you store with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoAPI (CNG) libraries.

The other options are incorrect:

AWS Codecommit is incorrect. AWS CodeCommit is mainly used for software version control, not for managing encryption keys.

Additional information:

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

AWS CodeDeploy is incorrect. AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises, and is not used for managing encryption keys.

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/kms/>

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

Question 29:

Skipped

Which of the following strategies help analyze costs in AWS?

- Using tags to group resources **(Correct)**
-
- Configuring Amazon Inspector to automatically analyze costs and email reports
-
- Using AWS CloudFormation to automate the deployment of resources
-
- Deploying resources of the same type in different regions

Explanation

Tags are key-value pairs that allow you to organize your AWS resources into groups. Implementing a tagging strategy will help you track usage and spending across different departments, applications, or Development/Production environments. For example, if you tag resources with an application name, you can track the total cost of a single application that runs on those resources.

You can use tags to:

- 1- Visualize information about tagged resources in one place.
- 2- View billing information using Cost Explorer and the AWS Cost and Usage report.
- 3- Create separate invoices for each project or work environment.

It is recommended that you use logical groupings of your resources that make sense for your infrastructure or business. For example, you could organize your resources by:

- Project

- Environment (Development - Testing - Production)
- Cost center
- Application
- Department

The other options are incorrect:

"Deploying resources of the same type in different regions" is incorrect. Deploying the same resource types in different regions will not help analyze costs in AWS, however it can help increase the reliability and resilience of your applications, especially if you have customers from different countries.

Note: When choosing an AWS Region, you should consider factors like proximity to end-users, data sovereignty, and costs.

"Using AWS CloudFormation to automate the deployment of resources" is incorrect. Automating the deployment of your resources through scripts allows you to build and rebuild your infrastructure and applications, without having to perform manual actions or write custom scripts, enabling configuration compliance and faster troubleshooting.

"Configuring Amazon Inspector to automatically analyze costs and email reports" is incorrect. Amazon inspector is not used for analyzing costs. It is a security assessment service for your applications.

References:

https://docs.aws.amazon.com/general/latest/gr/aws_tagging.html

Question 30:

Skipped

What is the main benefit of the AWS Storage Gateway service?



It provides physical devices to migrate data from on premises to AWS



It provides hardware-based key storage for regulatory compliance



It allows integration of on-premises IT environments with Cloud Storage

(Correct)



It automates the process of building, maintaining, and running ETL jobs

Explanation

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration between your on-premises IT environment and the AWS storage infrastructure.

AWS Storage Gateway supports four key hybrid cloud use cases:

- (1) Provide on-premises applications low latency access to data stored in AWS.
- (2) Migrate on-premises data to AWS, while maintaining fast local access to recently accessed data.
- (3) Optimize data transfer to AWS by sending only changed data, and compressing data.
- (4) Reduce on-premises storage with cloud-backed file shares.

The other options are incorrect:

"It automates the process of building, maintaining, and running ETL jobs" is incorrect. AWS Storage Gateway is not used for building and running ETL jobs. The name of the service that performs this function is AWS Glue.

ETL stands for "Extract, Transform, and Load" which is the process of collecting data from various sources (from different databases for example), transform the data

depending on business rules/needs (This step helps in preparing the data for analytics and decision making) and load the data into a destination database, often a data warehouse.

AWS Glue is a fully-managed, Extract, Transform, and Load (ETL) service that automates the time-consuming steps of data preparation for analytics. AWS Glue crawls your data sources, identifies data formats, and suggests schemas and transformations. After transforming the data, AWS Glue loads the data into your data warehouse or data lake for regular reporting and analysis. By storing data in a data warehouse or data lake, you integrate information from different parts of your business and provide a common source of data for decision making.

"It provides physical devices to migrate data from on premises to AWS" is not correct. AWS Storage Gateway does not provide physical devices to migrate data from on premises to AWS. The name of the service that performs this function is AWS Snowball.

"It provides hardware-based key storage for regulatory compliance" is incorrect. AWS Storage Gateway does not provide hardware-based key storage. The name of the service that performs this function is AWS CloudHSM.

The AWS CloudHSM service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are designed and validated to government standards for secure key management. HSM is a piece of hardware — a dedicated appliance that provides secure key storage and a set of cryptographic operations within a tamper-resistant enclosure. CloudHSM allows you to securely generate, store, and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

References:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

Question 31:

Skipped

Where can AWS account owners get a list of all users in their account, including the status of their AWS credentials?

- IAM Credential Report **(Correct)**
- AWS CloudTrail Trails
- AWS Artifact reports
- AWS Cost and Usage Report

Explanation

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the AWS Management Console, the AWS SDKs, and Command Line Tools.

You can use credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password and access key rotation. You can provide the report to an external auditor, or grant permissions to an auditor so that he or she can download the report directly.

The other options are incorrect:

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

"AWS Cost and Usage Report" is incorrect. The AWS Cost and Usage Report enables customers to access detailed information related to their AWS costs and usage.

"AWS CloudTrail trails" is incorrect. AWS CloudTrail is a service that logs all API calls related to your account.

References:

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

Question 32:

Skipped

You are using several on-demand EC2 Instances to run your development environment. What is the best way to reduce your charges when these instances are not in use?

-
-

Stopping the instances

(Correct)

-
-

Deleting all EBS volumes attached to the instances

-
-

You cannot minimize charges for on-demand instances

-
-

Terminating the instances

Explanation

AWS doesn't charge usage for a stopped instance, or data transfer fees. For a stopped instance AWS will only charge you for EBS storage volumes attached to the instances.

The other options are incorrect:

"Deleting all EBS volumes attached to the instances" is incorrect. This option is incorrect because you will lose the data on the EBS volumes in your development environment.

"Terminating the instances" is incorrect. If you terminate the instances without taking an image (AMI) of them, you will lose their data.

"You cannot minimize charges for on-demand instances" is incorrect. You can minimize charges by stopping the instances when you do not need them.

References:

<https://aws.amazon.com/ec2/pricing/on-demand/>

Question 33:

Skipped

You have just set up your AWS environment and have created six IAM user accounts for the DevOps team. What is the AWS recommendation when granting permissions to these IAM accounts?

- Attach a separate IAM policy for each individual account
 - Apply the Principle of Least Privilege
- (Correct)**
- Create six different IAM passwords

- ○

For security purposes, you should not grant any permission to the DevOps team

Explanation

The Principle of Least Privilege (PoLP, also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose. For example, a user account for the sole purpose of creating backups does not need to install software: hence, it has rights only to run backup and backup-related applications. Any other privileges, such as installing new software, are blocked.

The other options are incorrect:

"For security purposes, you should not grant any permission to the DevOps team" is incorrect. Each user should have the necessary permissions to do their assigned job. This will not impact the security of your account (if done correctly).

"Attach a separate IAM policy for each individual account" is incorrect. It is recommended to create an IAM group for each team and attach the required policies to the group. This way, if there is a change, you can simply apply it to that group not the individual accounts.

"Create six different IAM passwords" is incorrect. Passwords are not related to granting permissions. User names and passwords are used to authenticate users when logging into the AWS management console.

References:

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

Question 34:

Skipped

Which of the following will affect how much you are charged for storing objects in S3? (Choose TWO)

-

The number of Access Control Lists (ACLs) attached to your S3 buckets

-

Creating and deleting S3 buckets

-

The total size in gigabytes of all objects stored

(Correct)

-

Using default encryption for any number of S3 buckets

-

The storage class used for the objects stored

(Correct)

Explanation

S3 pricing is based on four factors:

- 1) Total amount of data (in GB) stored on S3
- 2) Storage class (S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access, S3 One Zone-IA, S3 Glacier, or S3 Glacier Deep Archive)
- 3) Amount of data transferred out of AWS from S3
- 4) Number of requests to S3

The other options are incorrect:

"The number of Access control lists (ACLs) attached to your S3 buckets" is incorrect. Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. **You can use ACLs to grant basic read/write permissions to other AWS accounts.** When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify that the requester has the necessary access permissions. This option is incorrect because there is no additional charge for using Amazon S3 ACLs.

Note: Amazon S3 ACLs are different than Network ACLs. A network access control list (Network ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

"Using default encryption for any number of S3 buckets" is incorrect. There are no extra charges for using default encryption for S3 buckets.

"Creating and deleting S3 buckets" is incorrect. Creating or deleting S3 buckets is free but you will be charged for data that you store in those buckets.

"The number of EBS volumes attached to your instances" is incorrect. Amazon EBS is a different AWS storage service. Amazon EBS is a block level storage service that provides storage volumes for use with Amazon EC2 and Amazon RDS.

References:

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

<https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html>

Question 35:

Skipped

Which of the following are use cases for Amazon EMR? (Choose TWO)

-

Enables you to move Exabyte-scale data from on-premises datacenters into AWS

- Enables you to easily run and scale Apache Spark, Hadoop, and other Big Data frameworks

(Correct)

- Enables you to easily run and manage Docker containers
- Enables you to analyze and process extremely large amounts of data in a timely manner

(Correct)

- Enables you to backup extremely large amounts of data at very low costs

Explanation

Amazon Elastic Map Reduce (Amazon EMR) is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. It utilizes a hosted Hadoop framework running on the web-scale infrastructure of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3).

Amazon EMR is ideal for problems that necessitate the fast and efficient processing of large amounts of data. EMR securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

Amazon EMR lets you focus on crunching or analyzing your data without having to worry about time-consuming set-up, management or tuning of Hadoop clusters or the compute capacity upon which they sit.

The other options are incorrect:

"Enables you to backup extremely large amounts of data at very low costs" is incorrect. EMR is not a storage service. Amazon EMR is a web service that enables you to process vast amounts of data across dynamically scalable Amazon EC2 instances. You can use Amazon Glacier or Amazon Glacier Deep Archive to backup large amounts of data at very low costs.

"Enables you to move Exabyte-scale data from on-premises datacenters into AWS" is incorrect. AWS Snowmobile is the service that can be used to transfer Exabyte-scale data from on-premises datacenters into AWS.

"Enables you to run and manage Docker containers" is incorrect. Amazon Elastic Container Service (ECS) is the service that can be used to run and manage Docker containers in AWS.

References:

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

Question 36:

Skipped

A company experiences fluctuations in traffic patterns to their e-commerce website when running flash sales. What service can help the company dynamically match the required compute capacity to handle spikes in traffic during flash sales?

-
-
-

AWS Auto Scaling

(Correct)

-
-
-

Amazon Elastic File System

-
-
-

Amazon Elastic Compute Cloud

-
-
-

Amazon ElastiCache

Explanation

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, you maintain optimal application performance and availability, even when workloads are periodic, unpredictable, or continuously changing. When demand spikes, AWS Auto Scaling automatically increases the compute capacity, so you maintain performance. When demand subsides, AWS Auto Scaling automatically decreases the compute capacity, so you pay only for the resources you actually need.

The other options are incorrect:

"Amazon Elastic Compute Cloud" is incorrect. Amazon Elastic Compute Cloud (EC2) is a service that provides compute capacity in the cloud.

"Amazon Elastic File System" is incorrect. Amazon Elastic File System (Amazon EFS) provides fully managed elastic **NFS file system** for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

"Amazon ElastiCache" is incorrect. Amazon ElastiCache is used to improve the performance of your existing apps by retrieving data from high throughput and low latency in-memory data stores.

References:

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

Question 37:

Skipped

Which of the following can help secure your sensitive data in Amazon S3? (Choose TWO)

-

Enable S3 Encryption

(Correct)

-

With AWS you do not need to worry about encryption

-

Delete the encryption keys once your data is encrypted

-

Delete all IAM users that have access to S3

-

Encrypt the data prior to uploading it

(Correct)

Explanation

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon data centers). You can protect data in transit by using SSL/TLS or by using client-side encryption.

Also, you have the following options of protecting data at rest in Amazon S3.

1- Use Server-Side Encryption – You configure Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

2- Use Client-Side Encryption – You can encrypt your data on the client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

The other options are incorrect:

"Delete the encryption keys once your data is encrypted" is incorrect. These keys are required to perform the decryption process.

"With AWS you do not need to worry about encryption" is incorrect. AWS does not encrypt the customer data automatically unless it is configured to do so. The customer is responsible for everything related to their data - access management, encryption, validation, lifecycle management, etc.

"Delete all IAM users that have access to S3" is incorrect. Instead of deleting your IAM users, you should restrict access to the S3 buckets using IAM policies.

References:

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

Question 38:

Skipped

Which of the below options is true of Amazon VPC?

-

AWS Customers have complete control over their Amazon VPC virtual networking environment

(Correct)

-

AWS is responsible for all the management and configuration details of Amazon VPC

-

Amazon VPC allows customers to control user interactions with all other AWS resources

-

Amazon VPC helps customers to review their AWS architecture and adopt best practices

Explanation

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, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

The other options are incorrect:

"Amazon VPC helps customers to review their AWS architecture and adopt best practices" is incorrect. Amazon VPC does not perform this function. The AWS Well-Architected Tool is the service that helps AWS Customers review their workloads against current AWS best practices and provides advice on how to architect their workloads for the cloud.

Note: What is a workload in AWS? A workload is the collection of resources and code that make up a cloud application.

"Amazon VPC allows customers to control user interactions with all other AWS resources" is incorrect. Amazon VPC does not allow customers to control user interactions with all other AWS resources. AWS IAM is the service that allows customers to perform this function.

"AWS is responsible for all the management and configuration details of Amazon VPC" is incorrect. AWS Customers are responsible for all the management and configuration details of Amazon VPC, not AWS.

References:

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

Question 39:

Skipped

Which service can you use to route traffic to the endpoint that provides the best application performance for your users worldwide?

-

AWS DAX Accelerator

-

AWS Global Accelerator

(Correct)

-

AWS Transfer Acceleration

-

AWS Data Pipeline

Explanation

AWS Global Accelerator is a networking service that improves the availability and performance of the applications that you offer to your global users. Today, if you deliver applications to your global users over the public internet, your users might face inconsistent availability and performance as they traverse through multiple public networks to reach your application. These public networks can be congested and each hop can introduce availability and performance risk. AWS Global Accelerator uses the highly available and congestion-free AWS global network to direct internet traffic from your users to your applications on AWS, making your users' experience more consistent. To improve the availability of your application, you must monitor the health of your application endpoints and route traffic only to healthy endpoints. AWS Global Accelerator improves application availability by continuously monitoring the health of your application endpoints and routing traffic to the closest healthy endpoints.

The other options are incorrect:

AWS Transfer Acceleration is incorrect. Amazon S3 Transfer Acceleration is used to enable fast transfers of files over long distances between your client and an S3 bucket. You might want to use Transfer Acceleration on a bucket for various reasons, including the following: 1- You have customers that upload to a centralized bucket from all over the world. 2- You transfer gigabytes to terabytes of data on a regular basis across continents. 3- You are unable to utilize all of your available bandwidth over the Internet when uploading to Amazon S3.

AWS DAX Accelerator is incorrect. Amazon DynamoDB Accelerator (DAX) is an in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second.

AWS Data Pipeline is incorrect. AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals. AWS Data Pipeline helps you easily create complex data processing workloads that are fault tolerant, repeatable, and highly available. With AWS Data Pipeline, you can regularly access your data where it's stored, transform and process it at scale, and efficiently transfer the results to AWS services such as Amazon S3, Amazon RDS, Amazon DynamoDB, and Amazon EMR.

References:

<https://d0.awsstatic.com/whitepapers/aws-overview.pdf>

Question 40:

Skipped

A media company has an application that requires the transfer of large data sets to and from AWS every day. This data is business critical and should be transferred over a consistent connection. Which AWS service should the company use?

- AWS VPN
- Amazon Comprehend
- AWS Snowmobile
- AWS Direct Connect

(Correct)

Explanation

AWS Direct Connect makes it easy for businesses to establish a dedicated network connection from their on-premises datacenters to AWS. Using AWS Direct Connect, customers can establish private connectivity between AWS and their datacenter, office, or co-location environment, which in many cases can reduce their network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

The other options are incorrect:

"AWS VPN" is incorrect. AWS Site-to-Site VPN provides an **internet-based connection** that enables customers to connect their on-premises network or branch office site to AWS. Internet-based connectivity can have **unpredictable performance** and despite being encrypted, can present security concerns.

AWS Direct Connect bypasses the public Internet and uses a standard Ethernet fiber-optic cable to establish a secure, dedicated, and **more consistent connectivity** from on-premises data centers into AWS.

AWS VPN is incorrect because transferring large data sets over the Internet can be time consuming and expensive. Additionally, AWS VPN is an internet-based connection and does not meet the requirement of consistent connectivity.

Additional information:

Unlike AWS Direct Connect, VPN Connections can be configured in **minutes** and are a good solution if customers have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

"AWS Snowmobile" is incorrect. AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS, including video libraries, image repositories, or even a complete data center migration. Customers can transfer up to 100 PetaBytes per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck.

"Amazon Comprehend" is incorrect. Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find meaning and insights in

text. Customers can use Amazon Comprehend to identify the language of the text, extract key phrases, places, people, brands, or events, understand sentiment about products or services, and identify the main topics from a library of documents. The source of this text could be web pages, social media feeds, emails, or articles. Amazon Comprehend is fully managed, so there are no servers to provision, and no machine learning models to build, train, or deploy.

References:

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

Question 41:

Skipped

For compliance and regulatory purposes, a government agency requires that their applications must run on hardware that is dedicated to them only. How can you meet this requirement?

- Use EC2 On-demand Instances
- Use EC2 Dedicated Hosts
- (Correct) Use EC2 Reserved Instances
- Use EC2 Spot Instances

Explanation

When you launch instances on a Dedicated Host, the instances run on a physical server that is dedicated for your use. While Dedicated instances also run on dedicated hardware, Dedicated Hosts provide further visibility and control by allowing you to place your instances on a specific, physical server. This enables you to deploy instances using configurations that help address corporate compliance and regulatory requirements.

Note:

Amazon EC2 purchasing options include: On-Demand, Savings Plans, Reserved Instances, Spot Instances, Dedicated Hosts and Dedicated instances.

Dedicated Instances also provides Hardware isolation. Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Your Dedicated instances are physically isolated at the host hardware level from instances that belong to other AWS accounts. However, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances.

The difference between *Dedicated Hosts* and *Dedicated Instances*:

1- Dedicated Instances guarantee that the instances will run on hardware that's dedicated to a single AWS account. But, as we mentioned above, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances. That is not the case with Dedicated Hosts. Dedicated Hosts allow you to control how instances are placed on a specific physical server, and you can consistently deploy your instances to the same physical server over time. For that reason, Dedicated Hosts is a better option to handle compliance and regulatory requirements in most scenarios.

2- Dedicated Hosts enable you to benefit from the Bring Your Own License (BYOL) model for almost every BYOL scenario, while only certain scenarios are supported by Dedicated Instances. The BYOL model enables AWS customers to use their **existing** server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server. Dedicated Hosts provide additional control over your instances and visibility into Host level resources and tooling that allows you to manage software that consumes licenses on a per-core or per-socket basis, such as Windows Server and SQL Server. This is why most BYOL scenarios are supported through the use of Dedicated Hosts, while only certain scenarios are supported by Dedicated Instances.

The other options are incorrect:

Spot, Reserved and On-demand Instances do not provide physical isolation for EC2 instances.

References:

<https://www.amazonaws.cn/en/ec2/dedicated-hosts/>

Question 42:

Skipped

You have a real-time IoT application that requires sub-millisecond latency. Which of the following services should you use?



Amazon Redshift



Amazon ElastiCache for Redis

(Correct)



Amazon Athena



AWS Cloud9

Explanation

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. Built on open-source Redis and compatible with the Redis APIs, ElastiCache for Redis works with your Redis clients and uses the open Redis data format to store your data. Your self-managed Redis applications can work seamlessly with ElastiCache for Redis without any code changes. ElastiCache for Redis combines the speed, simplicity, and versatility of open-source Redis with manageability, security, and scalability from Amazon to power the most demanding real-time applications in Gaming, Ad-Tech, E-Commerce, Healthcare, Financial Services, and IoT.

The other options are incorrect:

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

"Amazon Redshift" is incorrect. Amazon Redshift is a data warehouse service.

"Amazon Athena" is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. AWS customers can also use an Amazon S3 feature called **S3 Select** to query data on S3 using SQL commands; however, S3 Select can only be used to perform simple SQL queries on a single S3 Object.

References:

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

Question 43:

Skipped

The owner of an E-Commerce application notices that the compute capacity requirements vary heavily from time to time. What makes AWS more economical than traditional data centers for this type of application?

- AWS allows customers to launch powerful EC2 instances to handle spikes in load
- AWS allows customers to pay upfront to get bigger discounts
- AWS allows customers to launch and terminate EC2 instances based on demand

(Correct)

-

AWS allows customers to choose cheaper types of EC2 instances that best fit their needs

Explanation

On-Demand Instances have no contract commitment and can be launched (or terminated) as needed. With On-Demand instances, you pay for compute capacity by the hour or the second depending on which instances you run. This makes them ideal for applications with short-term or irregular workloads.

The other options are incorrect:

"AWS allows customers to choose cheaper types of EC2 instances that best fit their needs" is incorrect. In this example, the problem is not a matter of choosing the right instance type, the problem is that their application faces spikes in load.

Additional information:

AWS allows customers to choose from various types of EC2 Instances. Instance types comprise of various combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications.

"AWS allows customers to launch powerful EC2 instances to handle spikes in load" is incorrect. Provisioning powerful EC2 instances can handle spikes in load, but when the demand decreases you will still pay for those running instances.

Additional information:

Choosing the right instance type depends on your application's needs. In some cases, multiple small EC2 instances running in parallel can be more powerful and more economical than one large instance. For example, if a customer wants to transcode a large number of video files, AWS recommends using multiple small EC2 instances in parallel. If one instance is interrupted, the other instances can still complete their jobs.

"AWS allows customers to pay upfront to get bigger discounts" is incorrect. Paying upfront to get more discounts is possible using Reserved Instances. But this option is suitable only for applications that have a steady usage forecast for a period of a year or more.

References:

<https://aws.amazon.com/ec2/pricing/on-demand/>

Question 44:

Skipped

Your web application currently faces performance issues and suffers from long load times. Which of the following AWS services could help fix these issues and improve performance?



AWS Shield



AWS X-Ray

(Correct)



Amazon Detective



AWS Security Hub

Explanation

AWS X-Ray helps you identify performance bottlenecks. X-Ray's service maps let you see relationships between services and resources in your application in real time. You can easily detect where high latencies are occurring, visualize node and edge latency distribution for services, and then drill down into the specific services and paths impacting application performance.

The other options are incorrect:

Amazon Detective is incorrect. Amazon Detective is a security service that allows customers to analyze, investigate, and quickly identify the root cause of potential **security** issues or suspicious activities. Amazon Detective cannot detect **performance** issues.

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

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

References:

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

Question 45:

Skipped

You manage a blog on AWS that has different environments: development, testing, and production. What can you use to create a custom console for each environment to view and manage your resources easily?

-

AWS Resource Groups

(Correct)

-

AWS Management Console

-

AWS Placement Groups

- ○

AWS Tag Editor

Explanation

If you work with multiple resources in multiple environments, you might find it useful to manage all the resources in each environment as a group rather than move from one AWS service to another for each task. Resource Groups help you do just that. By default, the AWS Management Console is organized by AWS service. But with the Resource Groups tool, you can create a custom console that organizes and consolidates information based on your project and the resources that you use.

The other options are incorrect:

"AWS Management Console" is incorrect. AWS Management Console lets you access and manage individual AWS resources through a web-based user interface.

"AWS Tag Editor" is incorrect. AWS Tag Editor is used to add, edit, or delete tags from AWS resources.

"AWS Placement Groups" is incorrect. Placement Groups are logical groupings or clusters of EC2 instances within a single Availability Zone. Placement groups are recommended for applications that require low network latency, high network throughput, or both.

References:

<https://docs.aws.amazon.com/ARG/latest/APIReference/Welcome.html>

Question 46:

Skipped

Which of the following AWS services uses Puppet to automate how EC2 instances are configured?

- AWS OpsWorks
(Correct)
-
- AWS Quick Starts
-
- AWS CloudFormation
-
- AWS CloudTrail

Explanation

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.

The other options are incorrect:

AWS CloudTrail is incorrect. AWS CloudTrail is a service that logs all API calls related to your account.

AWS CloudFormation is incorrect. AWS CloudFormation is used to define and manage your infrastructure as code.

AWS Quick Starts is incorrect. AWS Quick Starts are automated reference deployments built by AWS solutions architects and partners to help you deploy popular technologies on AWS. Each Quick Start launches, configures, and runs the AWS compute, network, storage, and other services required to deploy specific workloads on AWS, using AWS best practices for security and availability.

References:

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

Question 47:**Skipped**

Who from the following will get the largest discount?

- A user who chooses to buy On-demand, Convertible, Partial upfront instances
 - A user who chooses to buy Reserved, Standard, All upfront instances
- (Correct)**
- A user who chooses to buy Reserved, Convertible, All upfront instances
 - A user who chooses to buy Reserved, Standard, No upfront instances

Explanation

Reserved instance types include:

- Standard RIs: These provide the most significant discount (up to 72% off On-Demand) and are best suited for steady-state usage.
- Convertible RIs: These provide a discount (up to 54% off On-Demand) and the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value.

Therefore, Standard RIs provides more discounts than Convertible RIs.

You can choose between three payment options when you purchase a Standard or Convertible Reserved Instance. With the All Upfront option, you pay for the entire Reserved Instance term with one upfront payment. With the Partial Upfront option, you make a low upfront payment and are then charged a discounted hourly rate for the instance for the duration of the Reserved Instance term. The No Upfront option does not require any upfront payment and provides a discounted hourly rate for the duration of the term.

* Remember that when you buy Reserved Instances, the larger the upfront payment, the greater the discount.

- The All Upfront option provides you with the largest discount.
- The Partial Upfront option provides fewer discounts than All Upfront.
- The No Upfront option provides you with the least discount.

The other options are incorrect:

"A user who chooses to buy Reserved, Convertible, All upfront instances" is incorrect. The Standard option provides more discounts than the Convertible option.

"A user who chooses to buy On-demand, Convertible, Partial upfront instances" is incorrect. Convertible is not an On-demand option.

"A user who chooses to buy Reserved, Standard, No upfront instances" is incorrect. "All upfront" provides more discounts than the "No-upfront" option.

References:

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

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-reservation-models/reserved-instances-payment-options.html>

Question 48:

Skipped

Which of the following services provide real-time auditing for compliance and vulnerabilities? (Choose TWO)

-

AWS Trusted Advisor

(Correct)

- Amazon MQ
- Amazon Redshift
- Amazon Cognito
- AWS Config

(Correct)

Explanation

Services like **AWS Config**, **Amazon Inspector**, and **AWS Trusted Advisor** continually monitor for compliance or vulnerabilities in your AWS environment which gives you a clear overview of which resources are in compliance, and which are not. With AWS Config rules you can also see if a component was out of compliance even for a brief period of time in the past, making both point-in-time and period-in-time audits very effective.

The other options are incorrect:

Amazon MQ is incorrect. Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud.

Amazon Redshift is incorrect. Amazon Redshift is a data warehousing service.

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

Cognito, you also have the option to authenticate users through social identity providers such as Facebook, Twitter, or Amazon, with SAML identity solutions, or by using your own identity system.

References:

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

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

Question 49:

Skipped

You want to create a backup of your data in another geographical location. Where should you create this backup?

- In another Local Zone
- In another Edge location
- In another Availability Zone
- In another Region

(Correct)

Explanation

A Region is a physical location around the world where AWS clusters data centers. AWS calls each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate Availability Zones within a geographic area. Unlike other cloud providers, who often define a region as a single data center, the multiple Availability Zones design of every AWS Region offers advantages for customers. Each Availability Zone has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple Availability Zones to achieve even greater fault-tolerance.

To save a backup to another geographical location, save it to a different AWS Region.

The other options are incorrect.

"In another Edge location" is incorrect. Edge locations are used in conjunction with the CloudFront service to cache and deliver content to global users with low latency. They are not used to store backups.

"In another Availability Zone" is incorrect. Availability Zones exist within a Region and are in the same geographic area.

"In another Local Zone" is incorrect. AWS Local Zones are not used to store backups. **A Local Zone is an extension of an AWS Region in geographic proximity to your users.** With AWS Local Zones, you can run highly-demanding applications that require single-digit millisecond latencies to your end-users, such as real-time gaming, hybrid migrations, AR/VR, and machine learning.

References:

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

Question 50:

Skipped

A company has infrastructure hosted in an on-premises data center. They currently have an operations team that takes care of identity management. If they decide to migrate to the AWS cloud, which of the following services would help them perform the same role in AWS?



Amazon Redshift

- AWS IAM
 - (Correct)
-
- AWS Federation
 -
-
- AWS Outposts

Explanation

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to access and use AWS resources.

The other options are incorrect:

"AWS Federation" is incorrect. Federation is an AWS feature that enables users to access and use AWS resources using their existing corporate credentials.

"Amazon Redshift" is incorrect. Amazon Redshift provides a fully managed data warehouse in the AWS Cloud.

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

References:

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

Question 51:**Skipped**

Select the services that are server-based: (Choose TWO)

- Amazon EMR
- **(Correct)** AWS Fargate
- Amazon DynamoDB
- Amazon RDS

(Correct)

- AWS Lambda

Explanation

Server-based services include: Amazon EC2, Amazon RDS, Amazon Redshift and Amazon EMR.

Serverless services include: AWS Lambda, AWS Fargate, Amazon SNS, Amazon SQS and Amazon DynamoDB.

References:

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

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

Question 52:

Skipped

Which of the following has the greatest impact on cost? (Choose TWO)

-

Data Transfer Out charges

(Correct)

-

Compute charges

(Correct)

-

The number of IAM roles provisioned

-

Data Transfer In charges

-

The number of services used

Explanation

The factors that have the greatest impact on cost include: Compute, Storage and Data Transfer Out. Their pricing differs according to the service you use.

The other options are incorrect:

"The number of services used" is incorrect. It does not matter how many AWS services you are using. Each AWS service has its own pricing details, and many of them are free to use.

"Data Transfer In charges" is incorrect. AWS does not charge any money for "Data Transfer In" for most services.

"The number of IAM roles provisioned" is incorrect. IAM and all of its features are free to use.

References:

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

Question 53:

Skipped

What can you use to assign permissions directly to an IAM user?

- IAM Role
- IAM Policy **(Correct)**
- IAM Group
- IAM Identity

Explanation

A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied.

Each policy consists of:

1- Principal:

Who needs access.

2- Action:

What action to allow or deny.

3- Resource:

Which resource to allow or deny the action on.

4- Effect:

What will be the effect when the user requests access - either allow or deny.

5- Condition:

Which conditions must be present for the policy to take effect. For example, you might allow access only to the specific S3 buckets if the user is connecting from a specific IP range or has used multi-factor authentication at login.

Note:

Permissions are granted to IAM identities (users, groups, and roles) to determine whether they are authorized to perform an action or not.

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. When you assume a role, it provides you with temporary security credentials for your role session. 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.

"IAM Group" is incorrect. You can use IAM groups to apply policies to users, however the policies are not directly attached to the IAM user. To assign permissions **directly** to an IAM user, attach an IAM policy to that user.

Additional information:

What is an IAM Group?

An IAM group is a collection of IAM users. 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 group called *Admins* and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to the group. If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to that 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 groups and add him or her to the appropriate new groups.

"IAM Identity" is incorrect. You create IAM Identities to provide authentication for people and processes in your AWS account. IAM identities include users, roles and groups.

References:

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

Question 54:

Skipped

Which of the following S3 storage classes is most appropriate to host static assets for a popular e-commerce website with stable access patterns?

-

S3 Intelligent-Tiering

-

S3 Standard

(Correct)

-

S3 Standard-IA

S3 Glacier Deep Archive

Explanation

S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

The other options are incorrect:

S3 Standard-IA is incorrect. S3 Standard Infrequent Access (S3 Standard-IA) is not for popular websites. S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA is ideal for long-term storage, backups, and as a data store for disaster recovery files.

S3 Intelligent-Tiering is incorrect. S3 Intelligent-Tiering is the ideal storage class for long-lived data with **access patterns that are unknown or unpredictable**. It is designed to optimize costs by automatically moving data to the most cost-effective access tier (Standard and Standard-IA), without performance impact or operational overhead.

S3 Glacier Deep Archive is incorrect. S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class that supports long-term retention and digital preservation for data that may be accessed once or twice in a year.

Note:

In S3, we can only host static websites, or **static assets of a dynamic website** (such as images, audio files, video files...etc).

A dynamic website relies on server-side processing and it uses server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting and

cannot be used to host dynamic websites. AWS has computing resources for hosting dynamic websites such as Amazon EC2 or Lambda.

References:

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

Question 55:

Skipped

An organization needs to build a financial application that requires support for ACID transactions. Which AWS database service is most appropriate in this case?

- RedShift
- RDS

(Correct)

- DMS
- CloudHSM

Explanation

In computer science, ACID (Atomicity, Consistency, Isolation, and Durability) is a set of properties of database transactions intended to guarantee validity even in the event of errors, power failures, etc. Amazon RDS is a fully-managed relational database service. It is a highly available and highly consistent database that supports ACID transactions. Basically, a transaction is one or more add, update, delete, or modify change to the database that must all be completed successfully or none of the steps should be executed. Transactional databases are useful when data integrity is important. If one of the steps in the transaction fail, then the steps must be rolled back to the state before any change was made to the database. An example of when you would need a transaction is when you make a banking transaction to move money from one account to another. If you successfully remove money from account A, but fail to add money to account B, then the transaction fails and the transaction must be rolled back so that the money is not taken from account A.

The other options are incorrect:

RedShift is incorrect. Amazon RedShift is a cloud data warehouse service.

DMS is incorrect. Amazon Database Migration Service (DMS) is used to migrate databases from your on-premises database system into AWS.

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

References:

<https://aws.amazon.com/relational-database/>

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

Question 56:

Skipped

Which of the following services gives you access to all AWS auditor-issued reports and certifications?

- AWS Config
-
- Amazon CloudWatch
-
- AWS CloudTrail
-

AWS Artifact

(Correct)

Explanation

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include AWS Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

The other options are incorrect:

"Amazon CloudWatch" is incorrect. Amazon CloudWatch is used to monitor AWS cloud resources.

"AWS CloudTrail" is incorrect. AWS CloudTrail is a service that provides visibility into user activity by logging all API calls related to your account. CloudTrail records important information about each API call, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. This information helps you to track changes made to your AWS resources and to troubleshoot operational issues.

"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 help with compliance 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, resource change tracking, and troubleshooting.

References:

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

Question 57:

Skipped

What kind of reports does AWS Cost Explorer provide by default?

- Reports about the results of AWS Trusted Advisor checks
 - Detailed AWS usage reports delivered directly to an Amazon S3 bucket
 - Reports about the utilization of Amazon EC2 Reserved Instances
- (Correct)**
- Reports about historical on-premises spending

Explanation

AWS Cost Explorer lets you dive deeper into your AWS cost and usage data to identify trends, pinpoint cost drivers, and detect anomalies. You can view data for up to the last 12 months, forecast how much you're likely to spend for the next 12 months, and get recommendations for what Savings Plans or Reserved Instances to purchase. AWS Cost Explorer reports include a breakdown of your top 5 cost-accruing AWS services, an analysis of your overall Amazon EC2 usage, an analysis of the total costs of your member accounts, and the Reserved Instance Utilization and Coverage reports.

The other options are incorrect:

"Detailed AWS usage reports delivered directly to an Amazon S3 bucket" is incorrect. The detailed AWS usage report that is delivered directly to an Amazon S3 bucket is called "AWS Cost & Usage Report", which is different than the reports provided by AWS Cost Explorer. The [AWS Cost & Usage Report](https://aws.amazon.com/artifact/) contains the most comprehensive set of AWS cost and usage data available. AWS delivers the AWS

Cost & Usage Report to whichever Amazon S3 bucket you specify during setup, and updates the reports at least once per day.

Using AWS Cost Management products, such as AWS Cost Explorer and AWS Budgets, you can gain greater visibility into your usage patterns and underlying cost drivers, as well as take action on any issues that you might see. However, if you are looking to build an enterprise-grade cost management solution in-house, you should strongly consider using the AWS Cost & Usage Reports as your foundation. The AWS Cost & Usage Report is best suited for organizations with complex cost management requirements, especially those who wish to establish dedicated query- or analytical-based systems in-house for cost reporting and analysis purposes.

"Reports about historical on-premises spending" is incorrect. AWS Cost Explorer does not provide reports about historical on-premises spending. AWS Cost Explorer provides you with interactive graphical reports designed to make it easier for you to view and analyze your historical spending on AWS.

"Reports about the results of AWS Trusted Advisor checks" is incorrect. AWS Cost Explorer does not provide reports about the results of AWS Trusted Advisor checks. These results can be found on the AWS Trusted Advisor dashboard. AWS Trusted Advisor is an online tool that offers a rich set of best practice checks and recommendations across five categories: **cost optimization, security, fault tolerance, performance, and service quotas.**

References:

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

Question 58:

Skipped

You are facing a lot of problems with your current contact center. Which service provides a cloud-based contact center that can deliver a better service for your customers?

-
-

AWS Elastic Beanstalk

-
-

Amazon Lightsail



Amazon Connect

(Correct)



AWS Direct Connect

Explanation

Amazon Connect is a cloud-based contact center solution. Amazon Connect makes it easy to set up and manage a customer contact center and provide reliable customer engagement at any scale. You can set up a contact center in just a few steps, add agents from anywhere, and start to engage with your customers right away. Amazon Connect provides rich metrics and real-time reporting that allow you to optimize contact routing. You can also resolve customer issues more efficiently by putting customers in touch with the right agents. Amazon Connect integrates with your existing systems and business applications to provide visibility and insight into all of your customer interactions.

The other options are incorrect:

"Amazon Lightsail" is incorrect. Amazon Lightsail provides a low-cost Virtual Private Server (VPS) in the cloud. Lightsail plans include everything you need to jumpstart your project – virtual machines, containers, databases, CDN, load balancers, SSD-based storage, DNS management, etc. – for a low, predictable monthly price.

"AWS Elastic Beanstalk" is incorrect. AWS Elastic Beanstalk makes it easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

"AWS Direct Connect" is incorrect. AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

References:

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

Question 59:

Skipped

Amazon RDS supports multiple database engines to choose from. Which of the following is not one of them?

- Oracle
- Microsoft SQL Server
- PostgreSQL
- Teradata

(Correct)

Explanation

Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. Amazon RDS is available on several database instance types - optimized for memory, performance or I/O - and provides you with **six database engines** to choose from, including **Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server**.

References:

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

Question 60:

Skipped

A company is hosting business critical workloads in an AWS Region. To protect against data loss and ensure business continuity, a mirror image of the current AWS environment should be created in another AWS Region. Company policy requires that the standby environment must be available in minutes in case of an outage in the primary AWS Region. Which AWS service can be used to meet these requirements?

-

CloudEndure Migration

-

AWS Glue

-

CloudEndure Disaster Recovery

(Correct)

-

AWS Backup

Explanation

CloudEndure Disaster Recovery is a disaster recovery solution that minimizes downtime and data loss by providing fast, reliable recovery of physical, virtual, and cloud-based servers into AWS Cloud. CloudEndure Disaster Recovery continuously replicates your machines (including operating system, system state configuration, databases, applications, and files) into a low-cost staging area in your target AWS account and preferred Region. In the case of a disaster (e.g., AWS Region outage, cyber-attack, power failure), you can instruct CloudEndure Disaster Recovery to automatically launch thousands of your machines in their fully provisioned state in minutes. This will help you recover quickly from disasters and achieve your business continuity goals.

The other options are incorrect:

"CloudEndure Migration" is incorrect. CloudEndure Migration is a highly automated lift-and-shift (rehost) solution that simplifies the process of migrating applications from physical, virtual, and cloud-based infrastructure, ensuring that they are fully operational in any AWS Region without compatibility issues.

"AWS Backup" is incorrect. AWS Backup can be used to copy backups to a different AWS Region, and recover from those backups in the new region in case of a disaster. But this Backup & Restore strategy requires hours to be implemented.

"AWS Glue" is incorrect. AWS Glue is a fully-managed, Extract, Transform, and Load (ETL) service that automates the time-consuming steps of data preparation for analytics.

Extract, Transform, and Load (ETL) is the process of **extracting** (collecting) data from various sources (from different databases for example), **transform** the data depending on business rules/needs (This step helps in preparing the data for analytics and decision making) and **load** the data into a destination database, often a data warehouse.

References:

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

Question 61:

Skipped

What are some key benefits of using AWS CloudFormation? (Choose TWO)

- It applies advanced IAM security features automatically
- It helps AWS customers deploy their applications without worrying about the underlying infrastructure
-

It compiles and builds application code in a timely manner

-

It allows you to model your entire infrastructure in just a text file

(Correct)

-

It automates the provisioning and updating of your infrastructure in a safe and controlled manner

(Correct)

Explanation

The benefits of using AWS CloudFormation include:

1- CloudFormation allows you to model your entire infrastructure in a text file. This template becomes the single source of truth for your infrastructure. This helps you to standardize infrastructure components used across your organization, enabling configuration compliance and faster troubleshooting.

2- AWS CloudFormation provisions your resources in a safe, repeatable manner, allowing you to build and rebuild your infrastructure and applications, without having to perform manual actions or write custom scripts. CloudFormation takes care of determining the right operations to perform when managing your stack, and rolls back changes automatically if errors are detected.

3- Codifying your infrastructure allows you to treat your infrastructure as just code. You can author it with any code editor, check it into a version control system, and review the files with team members before deploying into production.

4- CloudFormation allows you to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.

The other options are incorrect:

"It applies advanced IAM security features automatically" is incorrect. IAM features are not applied automatically. It is the customer's responsibility to manually apply the necessary IAM features to secure their AWS resources.

"It helps AWS customers deploy their applications without worrying about the underlying infrastructure" is incorrect. Services like AWS Elastic Beanstalk, Lambda, and Fargate allow you to deploy your applications without needing to worry about the underlying infrastructure. For example, with AWS Elastic Beanstalk, customers can simply upload their code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.

"It compiles and builds application code in a timely manner" is incorrect. AWS CloudFormation is not used to compile or build application code. The name of the service that performs this function is AWS CodeBuild.

References:

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

Question 62:

Skipped

Which AWS service collects metrics from running EC2 instances?

- AWS CloudTrail
- AWS CloudFormation
- Amazon Inspector
- Amazon CloudWatch

(Correct)

Explanation

Amazon CloudWatch is a monitoring service for 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.

The other options are incorrect:

"AWS CloudTrail" is incorrect. CloudTrail logs all API calls made to AWS services with credentials linked to your accounts.

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

References:

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

Question 63:

Skipped

Which statement is true in relation to the security of Amazon EC2?

-
- You can track all API calls using Amazon Athena
-

You should regularly patch the operating system and applications on your EC2 instances

(Correct)

- You should use instance store volumes to store login data
- You should deploy critical components of your application in the Availability Zone that you trust

Explanation

Amazon EC2 is not a managed service, AWS customers are responsible for patching the operating system and the applications they run on their instances.

AWS customers can automate this process by taking advantage of an AWS Systems Manager feature called "Patch Manager". AWS Systems Manager Patch Manager helps you **select and deploy operating system and software patches automatically** across large groups of Amazon EC2 or on-premises instances. Through patch baselines, you can set rules to auto-approve select categories of patches to be installed, such as operating system or high severity patches. Systems Manager helps ensure that your software is up-to-date and meets your compliance policies.

Note: The purpose of patching is to resolve functionality issues, improve security or add new features.

The other options are incorrect:

"You can track all API calls using Amazon Athena" is incorrect. Amazon Athena is an interactive query service that enables you to analyze data in Amazon S3 using standard SQL.

"You should deploy critical components of your application in the Availability Zone that you trust" is incorrect. All availability zones have the same level of security. They were designed using the same procedures and have the same

characteristics. If you want to protect critical components of your application, you should enable data encryption at rest and in transit.

"You should use instance store volumes to store login data" is incorrect. An instance store provides temporary storage for your instance. Data stored in instance store volumes is not persistent (The data will be lost if the instance stops, is terminated, or when hardware fails). To store login data, you should use a persistent storage service such as EBS.

References:

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

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

Question 64:

Skipped

What does the term "Economies of scale" mean?

-
-

It means that AWS will continuously lower costs as it grows

(Correct)

-
-

It means that you save more when you consume more

-
-

It means as more time passes using AWS, you pay more for its services

-
-

It means that you have the ability to pay as you go

Explanation

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

reduced the per GB storage price of S3 by 80% since the service was first introduced in 2006.

The other options are incorrect:

"It means that you save more when you consume more" is incorrect. It is correct that you can save more by using more but this describes the AWS tiered pricing not "Economies of scale".

"It means that you have the ability to pay as you go" is incorrect. It is correct that AWS gives you the ability to pay as you go so you can increase or decrease your spending as your company's requirements change, but this does not describe "Economies of scale".

"It means as more time passes using AWS, you pay more for its services" is incorrect. This statement should be "The more time passes using AWS, the less you pay for its services". This corrected statement now describes "Economies of scale". AWS Economies of Scale refers to the discounts that you get over time as AWS grows.

References:

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

Question 65:

Skipped

Which of the following is an available option when purchasing Amazon EC2 instances?

-

The ability to buy Dedicated Instances for up to 90% discount

-

The ability to bid to get the lowest possible prices

- ○ The ability to register EC2 instances to get volume discounts on every hour the instances are running
- ○ The ability to pay upfront to get lower hourly costs

(Correct)

Explanation

For Customers that can commit to using EC2 over a 1 or 3-year term, it is better to use Amazon EC2 Reserved Instances or AWS Savings Plans. Reserved Instances and AWS Savings Plans provide a significant discount (up to 72%) compared to On-Demand instance pricing.

1- Reserved Instances:

With EC2 Reserved Instances, you can save up to 72% over equivalent on-demand compute capacity. When you buy Reserved Instances, the larger the upfront payment, the greater the discount.

You can choose between three payment options when you purchase a Reserved Instance. With the All Upfront option, you pay for the entire Reserved Instance term with one upfront payment. This option provides you with the largest discount. With the Partial Upfront option, you make a low upfront payment and are then charged a discounted hourly rate for the instance for the duration of the Reserved Instance term. The No Upfront option does not require any upfront payment and provides a discounted hourly rate for the duration of the term.

2- AWS Savings Plans:

Savings Plans offer significant savings over On Demand, just like EC2 Reserved Instances, in exchange for a commitment to use a specific amount of compute power (measured in \$/hour) for a one or three year period. Savings Plans is available in 3 different payment options. The No Upfront option does not require any upfront payment, and your commitment will be charged purely on a monthly basis. The Partial Upfront option offers lower prices on Savings Plans. With this option you be charged at least half of your commitment upfront and the remaining will be charged

on a monthly basis. With the All Upfront option, you will receive the lowest prices and your entire commitment will be charged in one upfront payment.

The other options are incorrect:

"The ability to bid to get the lowest possible prices" is incorrect. AWS has eliminated "bidding" in the new AWS Spot instance pricing model. The way the new pricing model works is that you just pay the Spot price that's in effect for the current hour for the instances that you launch. It's that simple. Now you can request Spot capacity just like you would request On-Demand capacity, without having to spend time analyzing market prices or setting a bid price. In the new model, the Spot prices are more predictable, updated less frequently, and are determined by the long-term supply and demand for Amazon EC2 spare capacity, not bid prices. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.

An example to illustrate: If the current AWS Spot price is \$0.08 per hour and you set a maximum price of \$0.17, you'll pay \$0.08 and you will lose the instances if the AWS Spot price rises above \$0.17 or if capacity is no longer available.

"The ability to buy Dedicated Instances for up to 90% discount" is incorrect. The Amazon EC2 purchase option that provides up to 90% discount is Amazon EC2 Spot Instances.

"The ability to register EC2 instances to get volume discounts on every hour the instances are running" is incorrect. Volume-based discounting is a method by which the prices of units bought are lowered when large quantities are purchased. Volume Pricing or Tiered Pricing is not applied to EC2 hourly charges. Volume pricing is available only for storage and data transfer. The more storage and data transfer you use, the less you pay per gigabyte.

References:

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

<https://aws.amazon.com/savingsplans/faq/>

Question 1:

Skipped

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

- Amazon DynamoDB
- Amazon EBS **(Correct)**
- You can't run a database inside an Amazon EC2 instance
- Amazon RDS

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 2:

Skipped

Which statement is true in relation to security in AWS?

-

AWS is responsible for the security of your application

-

AWS manages everything related to EC2 operating systems

-

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

(Correct)

-

Server side encryption is the responsibility of AWS

Explanation

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

1- Using a managed database:

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

2- Installing a database software on Amazon EC2:

Instead of using a managed database, AWS customers can install any database software they want on Amazon EC2 and host their databases. In this case, **Customers**

are responsible for performing all of the necessary configuration and management tasks.

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

The other options are incorrect:

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

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

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

References:

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

Question 3:

Skipped

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

-

Enable AWS tiered-pricing before provisioning resources

- ○ Track the AWS charges that are incurred by the member accounts
- ○ Add the accounts to an AWS Organization and use Consolidated Billing

(Correct)

- ○ Try to remove unnecessary AWS accounts

Explanation

Consolidated billing has the following benefits:

- 1- One bill – You get one bill for multiple accounts.
- 2- Easy tracking – You can track each account's charges, and download the cost data in .csv format.
- 3- Combined usage – If you have multiple standalone accounts, your charges might decrease if you add the accounts to an organization. AWS combines usage from all accounts in the organization to qualify you for volume pricing discounts.
- 4- No extra fee – Consolidated billing is offered at no additional cost.

The other options are incorrect:

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

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

"Enable AWS tiered-pricing before provisioning resources" is incorrect. AWS tiered-pricing is applied for every AWS account regardless of whether it is part of an organization or not. With AWS, you can get volume-based

discounts and realize important savings as your usage increases. For services such as S3 and data transfer OUT from EC2, pricing is tiered, meaning the more you use, the less you pay per GB. But if you have multiple AWS accounts, you can achieve even more discounts by adding them to an Organization and enable consolidated billing (because in that case, AWS will treat all the accounts as one account).

References:

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

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

Question 4:

Skipped

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

- Amazon Macie
 - AWS Systems Manager Patch Manager
 - AWS Security Hub
 - AWS Control Tower
- (Correct)**

Explanation

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

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

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

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

The other options are incorrect:

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

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

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

References:

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

Question 5:

Skipped

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

- Provide an in-memory data storage service

(Correct)

- Provide a Chef-compatible cache to speed up application response
- Distribute requests to multiple instances
- Stream desktop applications from the cloud to user devices
- Improve web application performance

(Correct)

Explanation

Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory data store, instead of relying entirely on slower disk-based databases. Querying a database is always

slower and more expensive than locating a copy of that data in a cache. By caching (storing) common database query results, you can quickly retrieve the data multiple times without having to re-execute the query.

The other options are incorrect:

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

Interactively streaming your application from the cloud provides several benefits:

- 1- Instant-on: Streaming your application with Amazon AppStream 2.0 lets your users start using your application immediately, without the delays associated with large file downloads and time-consuming installations.
- 2- Remove device constraints: You can leverage the compute power of AWS to deliver experiences that wouldn't normally be possible due to the GPU, CPU, memory, or physical storage constraints of local devices.
- 3- Multi-platform support: You can take your existing applications and start streaming them to a computer without any modifications.
- 4- Easy updates: Because your application is centrally managed by Amazon AppStream 2.0, updating your application is as simple as providing a new version of your application to Amazon AppStream 2.0.

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

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

References:

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

Question 6:

Skipped

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



Amazon DocumentDB



Amazon RDS

(Correct)



Amazon DynamoDB



AWS Outposts

Explanation

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

The other options are incorrect:

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

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

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

References:

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

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

Question 7:

Skipped

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

-
- AWS CodeCommit
- (Correct)**
-
- Amazon CodeGuru
-
- AWS CodePipeline
-

AWS X-Ray

Explanation

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

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

The other options are incorrect:

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

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

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

References:

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

Question 8:

Skipped

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

-

Distributing requests to multiple volumes

-

Deleting unused Bucket ACLs

-

Using reservations

-

Deleting unnecessary snapshots

(Correct)

-

Changing the type of the volume

(Correct)

Explanation

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

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

1- Delete Unattached Amazon EBS Volumes:

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

2- Resize or Change the EBS Volume Type:

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

3- Delete Stale Amazon EBS Snapshots:

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

The other options are incorrect:

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

Note: You have three options to control access to an Amazon S3 Bucket:

1- IAM Policies

2- Bucket Policies

3- Bucket ACLs

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

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

References:

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

Question 9:

Skipped

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

- Savings Plans
- Reserved Instances
- Spot Instances
- On-Demand Instances

(Correct)

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 10:

Skipped

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

-
-

AWS Acceptable Use Policy

(Correct)

-
-

AWS Service Control Policies (SCPs)

-
-

AWS Budgets

-
-

AWS Artifact

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 11:

Skipped

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

-
- Amazon Simple Storage Service
-
- AWS CodeCommit
-
- Amazon CodeGuru
-

AWS Elastic Beanstalk

(Correct)

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 12:

Skipped

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



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

(Correct)



Notifies AWS customers about abuse events once they are reported



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



Helps AWS customers identify the root cause of potential security issues

Explanation

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

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

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

The other options are incorrect:

"Helps AWS customers identify the root cause of potential security issues" is incorrect. Amazon Detective is the service that helps AWS customers analyze,

investigate, and quickly identify the root cause of potential security issues or suspicious activities.

How does Amazon Detective differ from Amazon GuardDuty?

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

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

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

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

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

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

References:

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

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

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

Question 13:

Skipped

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

-

Replicate media assets to at least two availability zones

-

Store media assets in the region closest to your end users

(Correct)

-

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

-

Reduce the size of media assets using the Amazon Elastic Transcoder

-

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

(Correct)

Explanation

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

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

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

The other options are incorrect:

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

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

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

References:

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

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

Question 14:

Skipped

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

-

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

(Correct)

-

IAM users are more cost effective than IAM roles

-

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

(Correct)

-

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

-

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

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 15:

Skipped

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

- Your development team
- AWS

(Correct)

-

Your security team

-

Your internal DevOps team

Explanation

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

References:

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

Question 16:

Skipped

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

-

Proactive Technical Account Management

-

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

-

Consultative review and guidance based on your applications

-

Access to the full set of Trusted Advisor checks

(Correct)

-

AWS Support API

(Correct)

Explanation

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

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

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

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

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

Response times are as follows:

- General Guidance - < 24 hours
- System Impaired - < 12 hours
- Production System Impaired - < 4 hours
- Production System Down - < 1 hour

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

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

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

The other options are incorrect:

"Consultative review and guidance based on your applications" is incorrect. AWS support plans differ on what level of architectural support each of them provides. The AWS support plan that provides **consultative review and guidance** based on your applications is AWS **Enterprise** support.

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

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

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

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

References:

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

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

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

Question 17:

Skipped

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

-
- Cloud
- (Correct)**
-
- On-premises
-
- PaaS
-
- IaaS

Explanation

There are three Cloud Computing Deployment Models:

1- Cloud:

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

2- Hybrid:

A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud (On-premises data centers).

3- On-premises:

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

The other options are incorrect:

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

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

PaaS is incorrect. Platform as a Service (PaaS) removes the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

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

References:

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

Question 18:

Skipped

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

-

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

-

Manage your organization's payment methods

-

Control access to AWS services

(Correct)

-

Consolidate billing across multiple AWS accounts

(Correct)

-

Help organizations achieve their desired business outcomes with AWS

Explanation

AWS Organizations has five main benefits:

- 1) Centrally manage access policies across multiple AWS accounts.
- 2) Automate AWS account creation and management.
- 3) Control access to AWS services.
- 4) Consolidate billing across multiple AWS accounts.
- 5) Configure AWS services across multiple accounts.

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

** Consolidate billing across multiple AWS accounts: You can use AWS Organizations to set up a single payment method for all the AWS accounts in your organization

through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for Amazon EC2 and Amazon S3.

The other options are incorrect:

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

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

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

References:

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

Question 19:

Skipped

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

- Developer & Business Support
- Business & Enterprise Support
-

Developer & Enterprise Support

-

Basic & Developer Support

(Correct)

Explanation

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

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

References:

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

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

Question 20:

Skipped

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

-

Amazon S3

-

Amazon Rekognition

-

Amazon Elastic Transcoder

(Correct)

-
-

Amazon Pinpoint

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 21:

Skipped

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

-
-

Deploy your application across multiple EC2 instances

- ○

Deploy your application across multiple Availability Zones

(Correct)

- ○

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

- ○

Deploy the underlying application resources across multiple subnets

Explanation

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

The other options are incorrect:

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

This option is incorrect for two reasons:

- 1) It is not mentioned whether those instances will run in a single Availability Zone or multiple Availability Zones.
- 2) Deploying your application across multiple EC2 instances is costly and may not be necessary. The better alternative is to configure EC2 Auto Scaling to automatically add or remove instances and run the **required** number of instances **only**.

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

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

References:

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

Question 22:

Skipped

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

-
-

Use Amazon Aurora to forecast AWS spending based on usage

-
-

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

(Correct)

-
-

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

-
-

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

Explanation

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

your resource costs on your cost allocation report, to make it easier for you to categorize and track AWS costs across different departments.

The other options are incorrect:

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

Additional information:

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

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

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

References:

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

Question 23:

Skipped

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

- Network ACLs and Traffic Manager
- Security Groups and Network ACLs

(Correct)

- Security Groups and Internet Gateways
- Network ACLs and Subnets

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 24:

Skipped

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



WAF rules



Federation

(Correct)



Access keys



IAM Permissions

Explanation

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

AWS offers multiple options for federating your identities in AWS:

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

2- AWS Directory Service: AWS Directory Service for Microsoft Active Directory, also known as AWS Microsoft AD, uses secure Windows trusts to enable users to sign in to the AWS Management Console, AWS Command Line Interface (CLI), and

Windows applications running on AWS using their existing corporate Microsoft Active Directory credentials.

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

The other options are incorrect:

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

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

- Scripts that are likely to be malicious. Attackers embed scripts that can exploit vulnerabilities in web applications. This is known as cross-site scripting (XSS).
- Malicious requests from a set of IP addresses or address ranges.
- SQL code that is likely to be malicious. Attackers try to extract data from your database by embedding malicious SQL code in a web request. This is known as SQL injection.

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

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

References:

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

Question 25:

Skipped

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

-
- 100 PetaBytes
-
- 10 Exabytes
-
- 5 TeraBytes
-
- Virtually unlimited storage

(Correct)

Explanation

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

References:

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

Question 26:

Skipped

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

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

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

(Correct)

-

You have no responsibility for third-party software license costs

-

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

(Correct)

-

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

Explanation

AWS provides three pricing models:

- 1- Pay-as-you-go
- 2- Save when you reserve
- 3- Pay less by using more

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

The other options are incorrect:

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

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

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

References:

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

Question 27:

Skipped

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

- IAM user
- IAM role
- AWS account root user

(Correct)

- TAM
-

IAM group

Explanation

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

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

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

- 1- Change your account settings. This includes the account name, root user password, and email address.
- 2- Activate IAM access to the Billing and Cost Management console.
- 3- Close your AWS account.
- 4- Change your AWS Support plan or Cancel your AWS Support plan.
- 5- Register as a seller in the Reserved Instance Marketplace.
- 6- Configure an Amazon S3 bucket to enable MFA (multi-factor authentication) Delete. The AWS account owner (root account) configure MFA delete on a bucket to help ensure that the data in their bucket cannot be accidentally deleted.

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

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

The other options are incorrect:

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

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

References:

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

Question 28:

Skipped

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



Traceability



Accessibility



Elasticity



Durability

(Correct)

Explanation

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

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

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

Additional information:

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

The other options are incorrect:

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

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

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

References:

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

Question 29:

Skipped

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

-

Developer

-

Business

(Correct)

-

Enterprise

(Correct)

-

Standard

-

Premium

Explanation

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

The other options are incorrect:

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

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

References:

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

Question 30:

Skipped

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

-

Download all the attached policies in a safe place

-

Rotate all access keys

(Correct)

-

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

-

Delete all IAM accounts and recreate them

-

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

(Correct)

Explanation

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

To protect your AWS infrastructure you should:

- 1- Change the email address and the password of the root user account
- 2- Enable MFA on the root user account
- 4- Rotate (change) all access keys for all accounts
- 3- Change the user name and password of all IAM users

5- Enable MFA on all IAM user accounts

The other options are incorrect:

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

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

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

References:

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

Question 31:

Skipped

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

- Number of Volumes
- Storage Class
- Number of Requests

(Correct)

-

Traffic Distribution

(Correct)

-

Instance type

Explanation

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

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

- Traffic Distribution: Data transfer and request pricing varies across geographic regions, and pricing is based on the edge location through which your content is served.
- Requests: The number and type of requests (HTTP or HTTPS) made and the geographic region in which the requests are made.
- Data Transfer OUT: The amount of data transferred out of your Amazon CloudFront edge locations.

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

The other options are incorrect:

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

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

References:

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

Question 32:

Skipped

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

-

Use Serverless Computing whenever possible

(Correct)

-

Deploy your resources in another region

-

Use Elastic Load Balancing

-

Use Amazon EC2 Auto Scaling

(Correct)

-

Deploy your resources across multiple Availability Zones

Explanation

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

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

The other options are incorrect:

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

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

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

References:

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

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

Question 33:

Skipped

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

-

Per-second billing

- Provides cheaper options for purchasing Amazon EC2 on-demand instances
- Provides flexible pricing options that suit most customer needs

(Correct)

- Protects customers by performing periodic security checks on listed products

(Correct)

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

Explanation

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

The AWS Marketplace provides value to buyers in several ways:

- 1- It simplifies software licensing and procurement with flexible pricing options and multiple deployment methods. Flexible pricing options include free trial, hourly, monthly, annual, multi-year, and BYOL.
- 2- Customers can quickly launch pre-configured software with just a few clicks, and choose software solutions in AMI and SaaS formats, as well as other formats.
- 3- It ensures that products are scanned periodically for known vulnerabilities, malware, default passwords, and other security-related concerns.

The other options are incorrect:

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

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

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

References:

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

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

Question 34:

Skipped

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

-

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

(Correct)

-

Use manual monitoring techniques to protect your AWS resources

-

Enable real-time traceability

(Correct)

-

Never store sensitive data in the cloud

-

Scale horizontally to protect from failures

Explanation

There are seven design principles for security in the cloud:

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

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

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

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

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

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

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

The other options are incorrect:

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

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

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

References:

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

Question 35:

Skipped

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

-

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

(Correct)

-

They only require 1-2 days for setup and configuration

-

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

(Correct)

-

They are cheaper than all other EC2 options

-

They provide free capacity when testing your new applications

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 36:

Skipped

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

-
-

Amazon Macie

-
-

AWS KMS

(Correct)

-
-

AWS WAF

-
-

Amazon GuardDuty

Explanation

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

The other options are incorrect:

"Amazon GuardDuty" is incorrect. Amazon GuardDuty offers **threat detection** that enables you to continuously monitor and protect your AWS accounts and workloads. GuardDuty analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and

DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.

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

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

References:

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

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

Question 37:

Skipped

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

-

Improves Fault-Tolerance

(Correct)

-

Can be scaled manually in a shorter period of time

(Correct)

- Prevents unauthorized users from getting into your network
- Provides automatic data backups
- Provides your business with a seamless remote accessibility

Explanation

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

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

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

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

The other options are incorrect:

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

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

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

References:

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

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

Question 38:

Skipped

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

- Support plans
- Edge locations
- Regions

(Correct)



Transportation devices

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 39:

Skipped

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

- Use CloudWatch Alarms to monitor the CPU and alert when the CPU usage is $\geq 60\%$
- (Correct)**
- Set the AWS Config CPU threshold to 60% to receive a notification when EC2 usage exceeds that value
- Use SNS to monitor the utilization of the server
- Use CloudFront to monitor the CPU usage

Explanation

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

The other options are incorrect:

"Use SNS to monitor the utilization of the server" is incorrect. SNS is not used for monitoring. The service can be used in conjunction with CloudWatch to monitor and send notifications to your Email address. Using Amazon CloudWatch alarms, you can

set up metric thresholds and send alerts to Amazon Simple Notification Service (SNS). SNS can send notifications using e-mail, HTTP(S) endpoints, and Short Message Service (SMS) messages to mobile phones.

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

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

References:

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

Question 40:

Skipped

What should you consider when storing data in Amazon Glacier?

- Attach Glacier to an EC2 Instance to be able to store data
- Amazon Glacier only accepts data in a compressed format
- Glacier can only be used to store frequently accessed data and data archives
- Amazon Glacier does not provide immediate retrieval of data

(Correct)

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 41:

Skipped

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

-

EC2 launch type

(Correct)

- ○ Fargate launch type
- ○ Lambda launch type
- ○ Lightsail launch type

Explanation

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

The other options are incorrect:

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

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

References:

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

Question 42:

Skipped

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



Amazon Cognito



AWS Systems Manager Session Manager



AWS Cloud9



Amazon Route 53

(Correct)

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 43:

Skipped

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

- Amazon RDS
- Amazon Redshift Spectrum

(Correct)

- AWS Shield
- Amazon Comprehend
- Amazon Athena

(Correct)

Explanation

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

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

The other options are incorrect:

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

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

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

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

References:

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

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

Question 44:

Skipped

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

-

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

(Correct)

-

Ensure that all PCI DSS physical security requirements are met

-

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

-

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

-

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

(Correct)

Explanation

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

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

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

The other options are incorrect:

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

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

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

References:

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

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

Question 45:

Skipped

How does AWS help customers achieve compliance in the cloud?

- AWS has many common assurance certifications such as ISO 9001 and HIPAA
(Correct)
- AWS applies the most common Cloud security standards, and is responsible for complying with customers' applicable laws and regulations
- Many AWS services are assessed regularly to comply with local laws and regulations
- It's not possible to meet regulatory compliance requirements in the Cloud

Explanation

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

The other options are incorrect:

"AWS applies the most common Cloud security standards, and is responsible for complying with customers' applicable laws and regulations" is incorrect. In all

cases, customers operating in the cloud remain responsible for complying with applicable laws and regulations.

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

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

References:

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

Question 46:

Skipped

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

-
-
-

By configuring S3 Lifecycle Policies

-
-
-

By disabling S3 Cross-Region Replication (CRR)

-
-
-

By configuring S3 Bucket Policies

-
-
-

By enabling S3 Versioning

(Correct)

Explanation

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

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

The other options are incorrect:

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

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

"By configuring S3 Bucket Policies" is incorrect. A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. A Bucket Policy defines who can access a bucket, but does not help if an authorized user accidentally deleted objects in that bucket.

References:

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

Question 47:

Skipped

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

- Amazon Aurora
- **(Correct)** Amazon Route 53
- Amazon RDS for Oracle
- Instance Store
- S3

(Correct)

Explanation

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

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

Other Amazon RDS database engines (PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server) do not replicate data automatically. To protect from data loss when using any of these engines, you need to manually enable the Multi-AZ

feature. In a Multi-AZ Deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. If you encounter problems with the primary copy, Amazon RDS automatically switches to the standby copy to provide continued availability to the data.

The other options are incorrect:

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

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

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

References:

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

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

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

Question 48:

Skipped

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



Amazon Elastic Block Store



S3



AWS Storage Gateway



Amazon Elastic File System

(Correct)

Explanation

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

Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS that scale as a file system grows, with consistent low latencies. As a regional service, Amazon EFS is designed for high availability and durability storing data redundantly across multiple Availability Zones. With these capabilities, Amazon EFS is well suited to support a broad spectrum of use cases, including web serving and content management, enterprise applications, media and entertainment processing workflows, home directories, database backups, developer tools, container storage, and big data analytics workloads.

The other options are incorrect:

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

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

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

References:

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

Question 49:

Skipped

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

- Resource Configuration Management
- Awareness and Training
- Data center security controls

(Correct)

- Communications controls

-

Environmental controls

(Correct)

Explanation

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

As mentioned in the [AWS Shared Responsibility Model page](#), Inherited Controls are controls which a customer fully inherits from AWS such as physical controls and environmental controls.

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

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

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

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

The other options are incorrect:

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

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

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

References:

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

Question 50:

Skipped

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

-
-

AWS Tagging

(Correct)

-
-

AWS Service Catalog

-
-

AWS Directory Service

-
-

Amazon CloudWatch

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 51:

Skipped

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

-

AWS WAF

- AWS CloudHSM
- **(Correct)**
- AWS Shield
- AWS Certificate Manager

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 52:

Skipped

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

-

AWS TAM

-

AWS Classroom Training

-

AWS Security Blog

(Correct)

-

AWS Bulletins

(Correct)

-

AWS Support API

Explanation

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

The other options are incorrect.

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

"AWS Support API" is incorrect. AWS Support API is available only for AWS customers who have a **Business** or **Enterprise** support plan. The AWS Support

API provides **programmatic access** to AWS Support Center features to create, manage, and close support cases.

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

References:

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

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

Question 53:

Skipped

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

- It is a distinct location within a region that is insulated from failures in other Availability Zones
(Correct)
- It is a collection of data centers distributed in multiple countries
- It is a collection of Local Zones designed to be completely isolated from each other
- It is a logically isolated network of the AWS Cloud

Explanation

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

Note:

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

The other options are incorrect:

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

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

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

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

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

References:

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

Question 54:

Skipped

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

- Manages user access and encryption keys
- Distributes incoming traffic across multiple targets
- Controls what IP address ranges can connect to your database instance
- Deploys SSL/TLS certificates for use with your database instance

(Correct)

Explanation

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

References:

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

Question 55:

Skipped

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

- AWS Security Dashboard
-

AWS Billing Dashboard

-
- AWS Cost Dashboard
-
- AWS Service Health Dashboard

(Correct)

Explanation

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

References:

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

Question 56:

Skipped

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

-
- Amazon CloudWatch
- **(Correct)**
-
- Amazon Elastic MapReduce
-
- Amazon CloudSearch
-
- Amazon CloudHSM

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 57:

Skipped

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

-
- Resource Groups
-
- AWS Application Discovery service

- ○
AWS Marketplace

(Correct)

- ○
Amazon DevPay

Explanation

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

The other options are incorrect:

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

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

"Resource Groups" is incorrect. Resource Groups help you organize multiple AWS resources in groups. By default, the AWS Management Console is organized by AWS

service. But with the Resource Groups tool, you can create a custom console that organizes and consolidates information based on your project and the resources that you use.

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

References:

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

Question 58:

Skipped

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

-
-

Performing auditing tasks

-
-

Securing regions and edge locations

(Correct)

-
-

Monitoring AWS resources usage

-
-

Securing access to AWS resources

Explanation

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

All other options represent responsibilities of the customer.

References:

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

Question 59:

Skipped

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

- AWS Fargate
- Amazon EC2
- AWS Batch

(Correct)

- Lambda@Edge

Explanation

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

The other options are incorrect:

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

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

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

References:

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

Question 60:

Skipped

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

- Reliability
 - Operational Excellence
 - Security
 - Performance Efficiency
- (Correct)**

Explanation

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

The five Pillars of the AWS Well-Architected Framework: (IMPORTANT)

- 1- Operational Excellence
- 2- Security
- 3- Reliability
- 4- Performance Efficiency
- 5- Cost Optimization

The correct answer is: Performance Efficiency

The performance efficiency pillar includes the ability to use computing resources efficiently to meet system requirements. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

The other options are incorrect:

"Reliability" is incorrect. The reliability pillar includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. A resilient workload quickly recovers from failures to meet business and customer demand. Key topics include distributed system design, recovery planning, and how to handle change.

"Operational Excellence" is incorrect. The operational excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

"Security" is incorrect. The security pillar includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

References:

<https://aws.amazon.com/architecture/well-architected/>

Question 61:

Skipped

You have developed a web application targeting a global audience. Which of the following will help you achieve the highest redundancy and fault tolerance from an infrastructure perspective?

- Deploy the application in multiple Availability Zones in a single AWS region
- There is no need to architect for these capabilities in AWS, as AWS is redundant by default
- Deploy the application in a single Availability Zone
- Deploy the application in multiple Availability Zones in multiple AWS regions

(Correct)

Explanation

Since you are targeting a global audience, you should leverage AWS global regions to serve content to your users. The deployment option that gives you the highest redundancy is to deploy the application in multiple Availability Zones within multiple AWS regions. This redundancy will also increase the fault tolerance of the application because if there is an outage in a single Availability Zone, the other Availability Zones can handle requests.

Additional information:

It is important to understand that the AWS Cloud infrastructure is built around Regions and Availability Zones (AZs). A Region is a geographical location that contains multiple Availability Zones. Each AWS Region is designed to be completely isolated from the other AWS Regions. This achieves the greatest possible fault tolerance and stability.

An Availability Zone is a data center, or data centers, that are completely isolated from the other Availability Zones. Each AWS Region has at least two Availability Zones; most have three. Each Availability Zone is engineered to be independent from failures in other Availability Zones. Deploying your resources across multiple Availability Zones offer you the ability to operate production applications and databases that are more resilient, highly available, and scalable than would be possible from a single data center.

References:

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Question 62:

Skipped

Which of the following is NOT a benefit of using AWS Lambda?

-

There is no charge when your AWS Lambda code is not running

-

AWS Lambda runs code without provisioning or managing servers

-

AWS Lambda provides resizable compute capacity in the cloud

(Correct)

-

AWS Lambda can be called directly from any mobile app

Explanation

"AWS Lambda provides resizable compute capacity in the cloud" is not a benefit of AWS Lambda, so is the correct choice. AWS Lambda automatically runs your code without requiring you to adjust capacity or manage servers. AWS Lambda automatically scales your application by running code in response to each trigger. Your code runs in parallel and processes each trigger individually, scaling precisely with the size of the workload.

Other options represent benefits of AWS Lambda, so are not correct. AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume—there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service—all with zero administration. Just upload your code, and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services, or you can call it directly from any web or mobile app.

References:

<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

Question 63:

Skipped

Which of the following is a benefit of the "Loose Coupling" architecture principle?

- It allows for Cross-Region Replication
- It helps AWS customers reduce Privileged Access to AWS resources
- It allows individual application components or services to be modified without affecting other components

(Correct)

- It eliminates the need for change management

Explanation

As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components. This means that IT systems should be designed in a way that reduces interdependencies - a change or a failure in one component should not cascade to other components.

The AWS services that can help you build loosely-coupled applications include:

1- Amazon Simple Queue Service (Amazon SQS): Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS offers a reliable, highly-scalable hosted queue for storing messages as they travel between applications or microservices. It moves data between distributed application components and helps you decouple these components.

2- Amazon EventBridge (also called Amazon CloudWatch Events): Amazon EventBridge is a serverless event bus service that makes it easy for you to build event-driven application architectures. Amazon EventBridge helps you accelerate modernizing and re-orchestrating your architecture with decoupled services and applications. With EventBridge, you can speed up your organization's development process by allowing teams to iterate on features without explicit dependencies between systems.

3- Amazon SNS: Amazon SNS is a publish/subscribe messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Both Amazon SNS and Amazon EventBridge can be used to implement the publish-subscribe pattern. Amazon EventBridge includes direct integrations with software as a service (SaaS) applications and other AWS services. It's ideal for publish-subscribe use cases involving these types of integrations.

The other options are incorrect:

"It helps AWS customers reduce Privileged Access to AWS resources" is incorrect. This statement is related to the "Principle of Lease Privilege", not "Loose Coupling". Loose Coupling does not deal with access privileges.

"It allows for Cross-Region Replication" is incorrect. There is no relation between Cross-Region Replication and Loose Coupling. Cross-Region Replication (CRR) is an Amazon S3 feature that enables customers to replicate data across different AWS Regions; to minimize latency for global users and\or meet compliance requirements.

"It eliminates the need for change management" is incorrect. Loose Coupling does not eliminate the need for Change Management. Change Management is the process responsible for controlling the Lifecycle of all Changes made in an AWS account. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT Services. An erroneous configuration or misstep in a process can frequently lead to infrastructure or service disruptions. Creating and implementing a change management strategy will help reduce the risk of failure by monitoring all changes and rolling back failed changes.

Additional information:

AWS Config and AWS CloudTrail are change management tools that help AWS customers audit and monitor all resource and configuration changes in their AWS environment. AWS Config provides information about the changes made to a resource, and AWS CloudTrail provides information about who made those changes. These capabilities enable customers to discover any misconfigurations, fix them, and protect their workloads from failures.

References:

<https://aws.amazon.com/microservices/>

Question 64:

Skipped

What factors determine how you are charged when using AWS Lambda? (Choose TWO)

-

Number of volumes

-

Number of requests to your functions

(Correct)

-

Storage consumed

-

Placement groups

-

Compute time consumed

(Correct)

Explanation

With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the time it takes for your code to execute.

The other options are incorrect:

"Placement groups" is incorrect. Placement Groups are logical groupings or clusters of EC2 instances within a single Availability Zone.

"Storage consumed" and "Number of volumes" are incorrect. Lambda is not a storage service. It is a compute service to run your applications.

References:

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/how-aws-pricing-works.pdf> page 11

Question 65:

Skipped

Which of the following AWS services integrates with AWS Shield and AWS Web Application Firewall (AWS WAF) to protect against network and application layer DDoS attacks?

- Amazon CloudFront
- **(Correct)**
- AWS Secrets Manager
- Amazon EFS
- AWS Systems Manager

Explanation

Amazon CloudFront, AWS Shield, and AWS Web Application Firewall (AWS WAF) work seamlessly together to create a flexible, layered security perimeter against multiple types of attacks including network and application layer DDoS attacks. These services are co-resident at the AWS edge location and provide a scalable, reliable, and high-performance security perimeter for your applications and content.

All CloudFront distributions are defended by default against the most frequently occurring DDoS attacks that target your websites or applications with AWS Shield Standard. To defend against more complex attacks, you can add a flexible, layered security perimeter by integrating CloudFront with AWS Shield Advanced and AWS Web Application Firewall (AWS WAF).

Additional information:

AWS Shield provides always-on DDoS detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield

Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications.

The other options are incorrect:

"AWS Systems Manager" is incorrect. AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and execute actions on your groups of resources.

Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage your infrastructure at scale.

"AWS Secrets Manager" is incorrect. AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

"Amazon EFS" is incorrect. Amazon EFS is a storage service.

References:

<https://aws.amazon.com/cloudfront/>

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

<https://aws.amazon.com/shield/>