

## AWS Practical-2

Question 1: **Correct**

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

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

## References:

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

Question 2: **Correct**

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

•

Amazon EBS

•

Amazon Instance store

•

Amazon S3

**(Correct)**

•

Amazon SQS

## Explanation

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

**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 for storing images or videos. Amazon EBS is a block level storage that 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).

#### References:

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

Question 3: **Correct**

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

- Edge Locations
- 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.

**"Edge Locations" is incorrect.** Edge Locations are used by CloudFront to distribute content to end users with low latency.

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

#### References:

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

Question 4: **Correct**

**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?**

- 

AWS CloudTrail

- 

AWS CodePipeline

- 

Amazon Inspector

- 

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 5: **Incorrect**

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

- The ability of a system to recover gracefully from failure  
(Incorrect)
- The ability to monitor systems and improve supporting processes and procedures  
(Correct)
- The ability to manage datacenter operations more efficiently
- The ability to provision resources on-demand

#### 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 and to maintain that efficiency as demand changes and technologies 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 ability to provision resources on-demand" 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 6: **Correct**

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

•

AWS X-Ray

•

AWS Transit Gateway

•

AWS CloudTrail

**(Correct)**

- AWS Config

(Correct)

- Amazon Comprehend

### 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.

## References:

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

Question 7: **Correct**

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

- ☒ Managing the database settings  
(Correct)
- ☐ Installing the database software
- ☐ Patching the database software
- ☐ Performing backups
- ☒ Building the relational database schema  
(Correct)

## 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/>

Question 8: **Correct**

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

•

Amazon EFS

•

Amazon Glacier

•

Amazon S3

•

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 file system for Linux-based workloads for use with AWS Cloud services and on-premises resources. Amazon EFS cannot be used to store Amazon RDS DB instances.

**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 9: **Correct**

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

- 

Physical controls

(Correct)

- 

Patch management controls

- 

Database controls

- 

Awareness & Training

- 

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 10: **Correct**

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

•

CloudEndure

•

CloudWatch

•

CloudTrail

**(Correct)**

- 

## CloudFront

### 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 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 11: **Correct**

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

- Amazon EC2 instances

- Amazon LightSail

- AWS Lambda

(Correct)

- Amazon RDS 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 is a new offering from AWS to create a VPS (Virtual Private Server) on the cloud.

**"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 12: **Correct**

**How much data can you store in S3?**

- Storage capacity is virtually unlimited  
(Correct)
- You can store up to 1 PetaByte of data
- You can store up to 1 PetaByte of data, then you are required to pay an additional fee
- There is a soft limit of 100 TeraBytes for each AWS account

### Explanation

The total volume of data and number of objects you can store are unlimited.

## References:

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

Question 13: **Correct**

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

- EC2 instances will be billed on one hour increments, with a minimum of one day
- EC2 instances will be billed on one second increments, with a minimum of one minute  
**(Correct)**
- EC2 instances will be billed on one day increments, with a minimum of one month
- EC2 instances will be billed on one minute increments, with a minimum of one hour

### 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 or Ubuntu Instances and as a full hour for all other instance types.

### Examples for Linux\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 non-Linux\Ubuntu instances:

- 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 and Ubuntu

## References:

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

Question 14: **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 distribute content to global users with low latency

- 

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 traffic across multiple instances to reduce latency

(Correct)

## Explanation

The 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.** 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 15: **Incorrect**

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

- 

Use the Import/Export feature to move old files automatically to Amazon Glacier

(Incorrect)

- 

Use the right combination of storage classes based on different use cases

(Correct)

- Pick the right Availability Zone for your S3 bucket
- Move all the data stored in S3 standard to EBS

#### 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 16: Correct

**Which of the following AWS services are free to use? (Choose TWO)**



- 

Route53

- 

Auto-scaling

(Correct)

- 

Amazon EC2

- 

CloudFormation

(Correct)

- 

CloudWatch

### Explanation

The AWS Auto Scaling service itself is free to use, you only pay for the resources that Auto-scaling provisions on your behalf (e.g. scaling EC2 capacity up).

Additional information:

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 drops, AWS Auto Scaling will automatically remove any excess resource capacity so you avoid overspending. When demand increases, AWS Auto Scaling will automatically add capacity to maintain performance.

AWS CloudFormation is available at no additional charge, and you pay only for the AWS resources needed to run your applications.

Additional information:

AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion.

**The other options are incorrect:**

**CloudWatch is incorrect.** CloudWatch is not always free. You can get started with Amazon CloudWatch for free. Most AWS Services (EC2, S3, Kinesis, etc.) send metrics automatically for free to CloudWatch. Many applications should be able to operate within the free tier limits. But if you exceed those limits you will pay.

**Amazon EC2 is incorrect.** Amazon EC2 is free to try. AWS Free Tier includes 750 hours of Linux and Windows t2.micro instances each month for one year. If you exceed those limits you will pay.

**Route53 is incorrect.** Unlike many other services, there is no free tier usage with Route53. You have to pay for Route53 even if it is used with other free-tier services such as Amazon EC2 instances.

#### References:

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

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

Question 17: **Correct**

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

- 

Elastic Load Balancer

(Correct)

- 

CloudFormation

- 

AWS Direct Connect

- 

Network ACLs

- 

Amazon EC2 Auto Scaling

(Correct)

#### 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 18: **Correct**

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

- 

Amazon Inspector

(Correct)

- 

Amazon Kinesis

- 

Security groups

- 

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

Question 19: **Incorrect**

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

•

Amazon S3

•

Amazon EC2

(Correct)

•

AWS Lambda

(Correct)

•

Amazon CloudWatch

•

Amazon VPC

(Incorrect)

### 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 20: **Incorrect**

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

•

Amazon EFS

(Correct)

•

Amazon EMR

•

Amazon EBS

(Correct)

•

Amazon SNS

- 

Amazon ECS

(Incorrect)

### 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 21: **Incorrect**

**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?**

- 

Instance Password

- 

MFA

(Incorrect)

- 

Key pairs

- 

Access Keys

(Correct)

#### Explanation

**Access keys consist of two parts:** an **access key ID** and a **secret access key**. You use access keys to sign programmatic requests that you make to AWS if you use AWS CLI commands (using the SDKs) or using AWS API operations. 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/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

Question 22: **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?**

- 

Save when you reserve

(Correct)

-

Pay as you go

- 

Pay less by using more

- 

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://d1.awsstatic.com/whitepapers/aws\\_pricing\\_overview.pdf](https://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf)

Question 23: **Correct**

**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

- 

Remove single points of failure

**(Correct)**

-



Treat servers as fixed resources

- 

Automate wherever possible

(Correct)

- 

Always use Global Services in your architecture rather than Regional Services

#### 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://d1.awsstatic.com/whitepapers/architecture/AWS\\_Well-Architected\\_Framework.pdf](https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)

Question 24: **Correct**

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

- 

RDS PostgreSQL

- 

Amazon Neptune

- 

Amazon Aurora

**(Correct)**

- 

RDS Microsoft SQL Server

#### 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:**

**RDS PostgreSQL is incorrect.** RDS PostgreSQL is used to run PostgreSQL databases NOT MySQL databases.

**RDS Microsoft SQL Server is incorrect.** RDS Microsoft SQL Server is used to run Microsoft SQL Server databases NOT MySQL databases.

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

**References:**

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

Question 25: **Correct**

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

- Amazon Aurora
- **AWS WAF**  
(Correct)
- AWS IAM
- Amazon Cognito

#### 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 provides simple and Secure User Sign-Up, Sign-In, and Access Control.

#### References:

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

Question 26: **Incorrect**

**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 - No Upfront

(Incorrect)

- 

On-Demand instances

- 

Reserved instances - Partial Upfront

(Correct)

- 

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 27: **Correct**

**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?**

- 

IAM

- 

AMI

(Correct)

- 

An internet gateway

- 

EBS Snapshot

#### 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 28: **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

- 

Patching applications installed on Amazon EC2

(Correct)

- 

Controlling physical access to AWS Regions

- 

Protecting the confidentiality of data in transit in Amazon S3

(Correct)

- 

Ensuring that the underlying EC2 host is configured properly

(Incorrect)

### 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 29: **Correct**

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

- 

Security tokens

- 

A user name and password

(Correct)

- 

Access keys

- 

MFA

#### 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 to set a password policy for all IAM users to specify complexity requirements and mandatory rotation periods for their passwords.

You can use a 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.

**"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 30: **Correct**

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

•

Amazon EMR

(Correct)

•

Amazon SNS

•

Amazon SQS

•

Amazon MQ

#### 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 31: **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 DynamoDB
- Amazon SNS
- Amazon RDS  
(Correct)
- 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 32: **Incorrect**  
**Which statement is correct with regards to AWS service limits? (Choose TWO)**

- You can use the **AWS Trusted Advisor to monitor** your service limits  
(Correct)

- 

Each IAM user has the same service limits

(Incorrect)

- 

You can **contact AWS support to increase** the service limits

(Correct)

- 

There are no service limits on AWS

(Incorrect)

- 

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

#### Explanation

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.** You can find a full list of the AWS service limits on this page:

[https://docs.aws.amazon.com/general/latest/gr/aws\\_service\\_limits.html](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html)

**"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.

#### References:

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

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

<https://aws.amazon.com/premiumsupport/knowledge-center/manage-service-limits/>

Question 33: **Correct**

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

- Number of buckets
- Storage capacity  
(Correct)
- The Availability Zone where the instance is provisioned
- Instance type  
(Correct)
- Number of private IPs

#### Explanation

EC2 instance pricing varies depending on many variables:

- The buying option (On-demand, Reserved, Spot, Dedicated)
- Selected AMI
- Selected instance type
- Region
- Data Transfer in/out
- Storage 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. They do not vary based on which AZ they are hosted within a region.

**"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. You can have only one Elastic IP (EIP) address associated with a running instance at no charge.

**"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 similar to 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://aws.amazon.com/ec2/faqs/>

### Question 34: 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?

- 

Global reach

(Correct)

- 

Elasticity

(Incorrect)

- 

Data durability

-

## High availability

### 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 Zones 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 99.999999999% 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 35: **Correct**

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

- 

AWS Trusted Advisor

- 

Amazon Config

-

AWS Organizations

(Correct)

•

AWS WAF



### 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.

**"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 36: **Correct**

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

•

VPC Flow logs

•

NACL

- AWS X-Ray

- Security Groups

(Correct)

#### Explanation

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

**The other options are incorrect:**

**"NACL" is incorrect.** A network access control list (NACL) 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: NACLs act at the subnet level, but security groups act at the instance level.

**"AWS X-Ray" is incorrect.** AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.

**"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 NACLs 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.

**Security Groups, NACLs, 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_Security.html)

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

Question 37: **Correct**

**Which of the following enables you to monitor and collect log files from your Amazon EC2 instances?**

CloudWatch Logs

(Correct)

- AWS Storage Gateway
- AWS CloudTrail
- Amazon Inspector

#### Explanation

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.

**The other options are incorrect:**

**"AWS CloudTrail" is incorrect.** CloudTrail is used to log, continuously monitor user activity and API usage.

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

**"AWS Storage Gateway" is incorrect.** AWS Storage Gateway is a hybrid cloud storage service.

#### References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

Question 38: **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



- 

Amazon RDS

- 

AWS Identity and Access Management

(Correct)

- 

Network Access Control Lists

#### 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 39: **Incorrect**

**Which of the following is one of the benefits of AWS security?**

- 

Scales quickly with your AWS usage

(Correct)

- 

Increases Capital expenditure (CapEx)

-

Starts automatically once you upload your data

(Incorrect)

Free for AWS premium members

#### Explanation

Security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.

**The other options are incorrect:**

**"Free for AWS premium members" is incorrect.** Not all security features are free. For example Security Groups are free for all customers; however Amazon Inspector is not free.

**"Starts automatically once you upload your data" is incorrect.** AWS Security doesn't start automatically, you have to go on and set up how your data will be accessed and decide whether this data will be encrypted or not and so on.

**"Increases Capital expenditure (CapEx)" is incorrect.**

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.

#### References:

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

Question 40: **Correct**

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

Amazon Redshift

Amazon DynamoDB

- 

Amazon EC2

(Correct)

- 

Amazon RDS

#### 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 41: **Correct**

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

- 

AWS Console

- 

AWS Service Catalog

- 

AWS OpsWorks

- 

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 42: **Incorrect**

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

•

PaaS

•

IaaS

(Correct)

•

IaaS & SaaS

(Incorrect)

•

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 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 43: **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 scalable system

- ☐

She has properly built a fault tolerant system

(Correct)

- She has properly built an encrypted 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 expects that the website will be available and ready to accept his 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://d1.awsstatic.com/whitepapers/architecture/AWS\\_Well-Architected\\_Framework.pdf](https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)

Question 44: **Correct**

**What does Amazon Elastic Beanstalk provide?**

- A compute engine for Amazon ECS
- A PaaS solution to automate application deployment

(Correct)

- 

A NoSQL database service

- 

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

#### 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 45: **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?**

- 

AWS Snowball

- 

AWS WAF

- 

S3 Transfer Acceleration

(Correct)

- 

AWS Snowmobile

#### 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" correct.** 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 46: **Correct**

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

•

AWS Snowball

•

Amazon CloudFront

•

AWS Direct Connect

**(Correct)**

•

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 47: **Correct**

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

- Amazon Simple Storage Service
- AWS Storage Gateway
- Amazon Simple Email Service
- Amazon Simple Queue Service

**(Correct)**

#### 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 48: **Incorrect**

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

•

Dedicated hosting

•

Eliminating(REMOVE) Single Points of Failure (SPOFs)

(Correct)

•

Distributed infrastructure

(Correct)

•

Reserved Compute capacity

•

Virtualized compute resources

(Incorrect)

## 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 60 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 over-spending. 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 49: **Incorrect**

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

- 

Amazon Simple Storage Service

(Correct)

- 

Amazon Redshift

- 

AWS Snowball

- Amazon DynamoDB

(Correct)

- Amazon EBS

(Incorrect)

#### 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 99.99999999% 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 50: **Correct**

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

- 

Dynamic websites' assets

- 

Active archives

(Correct)

- 

Active databases

- 

Long-term analytic data

(Correct)

- 

Cached data

#### 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 51: **Correct**

Which of the following activities may help **reduce your AWS monthly costs**?

- Deploying your AWS resources across multiple Availability Zones
- **Enabling Amazon EC2 Auto Scaling for all of your workloads**  
(Correct)
- Using the AWS Network Load Balancer (NLB) to load balance the incoming HTTP requests
- Removing all of your Cost Allocation Tags

#### 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.

**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 three types of load balancers. You can select the appropriate load balancer based on your application needs. If you need to load balance HTTP requests, AWS recommends using the Application Load Balancer. For network/transport protocols (layer4 – TCP, UDP) load balancing, and for extreme performance/low latency applications, AWS recommends using Network Load Balancer. If your application is built within the EC2 Classic network then you should use Classic Load Balancer.

### References:

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

Question 52: **Incorrect**

**What does Amazon ElastiCache provide?**

•

A domain name system in the cloud

•

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

•

An Elcache compatible in-memory data store

**(Incorrect)**

•

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 53: **Correct**

**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?**

- 

Create a CDN using CloudFront, so that content is cached at Edge Locations close to and in Asia

(Correct)

[github.com/bvnaikum7](https://github.com/bvnaikum7)

- 

Migrate the application to a hosting provider in Asia

-



Recreate the website content

- 

Replicate the current resources across multiple Availability Zones within the same region

#### 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/cloudfront/>

Question 54: **Correct**

**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 EC2 Auto Recovery

- 

AWS Network Load Balancer

- 

AWS Auto Scaling

- 

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 three types of load balancers: 1- Application Load Balancer. 2- Network Load Balancer. 3- 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 55: **Correct**

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

- 

AWS Cloud9

- 

AWS Data Pipeline

- 

Amazon ECS

(Correct)

- 

AWS Personal Health Dashboard

### 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 56: **Correct**

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

•

Security Groups

**(Correct)**

•

AWS IAM

•

Network Access Control Lists

**(Correct)**

- AWS CloudHSM

- AWS Batch

### Explanation

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. A Network Access Control List (NACL) acts as a firewall for controlling traffic in and out of one or more subnets. Therefore, if they are configured properly, they can protect your instances from DDoS attacks.

### Additional information:

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

In addition to Security Groups and NACLs, 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 57: **Correct**

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

-

Securing global physical infrastructure

(Correct)

- 

Hardware patching

(Correct)

- 

Access permissions

- 

VPC security

- 

Encryption of EBS volumes

#### 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 in 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://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>

Question 58: **Correct**

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

•

AWS CloudTrail

•

AWS Cloud9

•

AWS Direct Connect

**(Correct)**

•

AWS VPN

**(Correct)**

•

AWS Artifact

## 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 (AWS VPN) provides an internet-based Site-to-Site connection that enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). A VPC VPN Connection utilizes IPSec to establish encrypted connectivity between your network and Amazon VPC over the Internet. 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 59: **Correct**

**Which AWS service uses Edge Locations to cache content?**

- 

AWS Direct Connect

- 

AWS KMS

- 

Amazon CloudFront

(Correct)

- 

Amazon Glacier

#### Explanation

Amazon CloudFront is a content caching service provided by AWS that uses Edge Locations (which are AWS data centers located all around the world) to reduce network latency when delivering content to end users.

**The other options are incorrect:**

**"Amazon Glacier" is incorrect.** Amazon Glacier is an Amazon S3 storage class.

**"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.

#### References:

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

Question 60: **Correct**

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

- 

Read Replicas

(Correct)

- 

Automatic patching



- Multi-AZ Deployment

(Correct)

- Edge Locations

- AWS Regions

#### 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-replicas/>

Question 61: **Correct**

**When using the AWS TCO tool, what information is required to calculate the potential savings of using AWS vs. on-premises?**

- The number of active databases
- The number of end users you are currently serving
- The number of on-premise applications
- The number of on-premise virtual machines

**(Correct)**

#### *Explanation*

The AWS TCO (Total Cost of Ownership) Calculator provides directional guidance on possible realized savings when using AWS. This tool is built on an underlying calculation model, that generates a fair assessment of value that a customer may achieve given the data provided by the user which includes the number of servers migrated to AWS, the server type, the number of processors per server and so on.

The AWS TCO tool only asks you about server and storage configuration details, but if you are going to perform the TCO analysis yourself, you should consider other factors such as cooling and power consumption, data center space, IT labor cost and so on.

The AWS TCO tool does not ask you to provide information about your current power and cooling consumption, data center space, IT labor costs. The AWS TCO tool estimates these costs based on specific assumptions for on-premises, co-location, and AWS environments.

To understand the TCO tool better, just go to <https://awstccalculator.com/>, enter some values for the fields presented, and then click "Calculate TCO" at the bottom.

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

***"The number of end users you are currently serving" is incorrect.*** The TCO Calculator doesn't ask for the number of end users you are currently serving. See <https://awstccalculator.com/>

**"The number of on-premise applications" is incorrect.** The TCO Calculator doesn't ask for the number of applications migrated to AWS. Also, what really matters is the size of your application and your business.

**"The number of active databases" is incorrect.** The TCO calculator asks for the number of servers that run your databases NOT the number of active databases.

#### References:

<https://aws.amazon.com/tco-calculator/>

Question 62: **Incorrect**

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

•

Amazon DynamoDB

•

Amazon Redshift

**(Correct)**

•

Amazon Kinesis

•

Amazon RDS

**(Incorrect)**

#### 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 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 63: **Incorrect**

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

- Installing software on EC2 instances
- Hardware maintenance  
(Correct)
- Configuring Access Control Lists (ACLs)
- Monitoring network performance  
(Incorrect)
- Creating hypervisors  
(Correct)

#### 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 64: **Correct**

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

•  
AWS Professional Services

•  
APN Technology Partners

•  
APN Consulting Partners

**(Correct)**

•  
AWS TAM

#### 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/>

Question 65: **Incorrect**

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

- 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  
(Incorrect)
- Ensure that the application runs on hardware from trusted vendors

### 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/>

@pvnakum  
@pvna

github.com/pvnakum7